

NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

BUSINESS MEETING AGENDA

The Washington Marriott at Metro Center
Salon A
775 12th Street, NW, Washington, DC 20005
July 12, 2011
1:30 PM – 4:30 PM EDT

- | | |
|---|--|
| I. OPENING OF MEETING | <i>Nancy J. Wong</i> , Designated Federal Officer (DFO), National Infrastructure Advisory Council (NIAC), Department of Homeland Security (DHS) |
| II. ROLL CALL OF MEMBERS | <i>Nancy J. Wong</i> , DFO, NIAC, DHS |
| III. OPENING REMARKS AND INTRODUCTIONS | NIAC Acting Chairman <i>Alfred R. Berkeley</i> , Chairman, Pipeline Trading Systems, LLC (former Vice Chairman, The NASDAQ Stock Market, Inc.)

<i>Sue Armstrong</i> , Deputy Assistant Secretary for Infrastructure Protection (IP), DHS |
| IV. APPROVAL OF JANUARY 2011 MINUTES | NIAC Acting Chairman <i>Alfred R. Berkeley</i> , Chairman, Pipeline Trading Systems, LLC (former Vice Chairman, The NASDAQ Stock Market, Inc.) |
| V. WORKING GROUP DELIBERATIONS
INFORMATION SHARING STUDY | <i>Alfred R. Berkeley</i> , Chairman, Pipeline Trading Systems, LLC (former Vice Chairman, The NASDAQ Stock Market, Inc.), NIAC Acting Chairman, Working Group Co-Chair and <i>Michael J. Wallace</i> , Former Vice Chairman and COO Constellation Energy, NIAC Member, Working Group Member |
| VI. PUBLIC COMMENT | <i>Nancy J. Wong</i> , DFO, NIAC, DHS |
| VII. CLOSING REMARKS | <i>Sue Armstrong</i> , Deputy Assistant Secretary, IP, DHS |
| VIII. ADJOURNMENT | NIAC Acting Chairman <i>Alfred R. Berkeley</i> , Chairman, Pipeline Trading Systems, LLC (former Vice Chairman, The NASDAQ Stock Market, Inc.) |

MINUTES

NIAC MEMBERS PRESENT IN WASHINGTON:

Mr. Alfred Berkeley, III; Lt. Gen. (ret.) Albert Edmonds; Ms. Margaret Grayson; Mr. David Kepler; Ms. Constance Lau; Mr. Greg Peters; Dr. Linwood Rose; Dr. Beverly Scott; Mr. Michael J. Wallace

NIAC MEMBERS ATTENDING VIA CONFERENCE CALL:

Mr. Jack Baylis; Mr. Gilbert Gallegos; Mr. Donald Knauss; Mr. James B. Nicholson; Mr. James Reid; Ms. Martha Wyrsh

MEMBERS ABSENT:

Mr. David Bronczek; Mr. Wesley Bush; Mr. David Grain; Mr. Philip Heasley; Commissioner Raymond Kelly; Mr. Thomas Noonan

SUBSTANTIVE POINTS OF CONTACT PRESENT IN WASHINGTON:

Mr. Gerald Buckwalter (for Mr. Wesley Bush); Ms. Katherine English (for Mr. David Kepler); Ms. Joan Gehrke (for Mr. James B. Nicholson); Ms. Robin Holliday (for Mr. Alfred Berkeley, III)

SUBSTANTIVE POINTS OF CONTACT ATTENDING VIA CONFERENCE CALL:

Ms. Frances Paulson (for Mr. Wesley Bush)

OTHER DIGNITARIES PRESENT:

Mr. Brian Kamoie, White House, National Security Staff, Senior Director for Preparedness Policy; Ms. Sue Armstrong, Deputy Assistant Secretary, IP, DHS; and Ms. Nancy Wong, DFO, NIAC, DHS

I. OPENING OF MEETING

Nancy J. Wong, DFO, NIAC, DHS

Ms. Nancy Wong, the DFO for the NIAC, called the meeting to order and welcomed all individuals, both in person and via teleconference, to the NIAC Quarterly Business Meeting. Ms. Wong introduced Acting Chairman Alfred Berkeley, Deputy Assistant Secretary for IP Sue Armstrong, Mr. Brian Kamoie of the National Security Staff, NIAC members and their staff, other Federal Government representatives, and members of the press and public in attendance.

Ms. Wong identified the NIAC as a presidentially appointed council, with its work directly related to Homeland Security Presidential Directive 7 (HSPD-7), which established a National policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks.

Ms. Wong provided a synopsis of the Council's formation, history, pertinent reports and studies produced, and positive feedback and reception of its products. She noted that in October 2009, The NIAC Charter was renewed by Executive Order 13511. This document outlines the role of the Council providing both the President of the United States and Secretary for DHS with advice on the security of critical infrastructure and key resources supporting the public and private sectors.

Ms. Wong reiterated the importance of the public and private sector partnership, which is exhibited in the Council and in the critical infrastructure environment, and on which the National economy and public safety depend. She noted that during the Council's 10 year history, 20 relevant studies have

been completed which have dealt with matters ranging from the cooperation and partnership between the public and private sectors to policies and strategies involving risk assessment, information sharing, and critical infrastructure and key resource protection impacting the public and private sectors of society.

II. ROLL CALL

Nancy J. Wong, DFO, NIAC, DHS

Ms. Wong called the roll and recorded attendance noting whether members were attending in person or via teleconference.

Upon completion of the roll call, Ms. Wong reminded members of the Council that the meeting is open to the public and that care should be taken if and when discussing issues of a sensitive matter. In addition, she explained that at the end of the meeting, there would be a public comment period, and though the NIAC had received no requests for public comments, the time would still be noted in the record. Ms. Wong then called the NIAC meeting to order; the second for 2011, and turned the proceedings over to Acting Chairman Berkeley.

III. OPENING REMARKS AND INTRODUCTIONS

*NIAC Acting Chairman Alfred R. Berkeley,
Chairman, Pipeline Trading Systems, LLC
(former Vice-Chairman, The NASDAQ
Stock Market, Inc.)*

Acting Chairman Berkeley thanked Ms. Wong and welcomed all attendees to the meeting. He recognized and thanked Deputy Assistant Secretary Armstrong and Mr. Kamoie for their attendance and invited Ms. Armstrong to make an opening statement.

Deputy Assistant Secretary Armstrong thanked Acting Chairman Berkeley and the members of the NIAC. She then went on to say that she looked forward to the deliberations on the *Information Sharing Study*. Ms. Armstrong stated that during the Council's 10 year history that it had issued a number of relevant and timely reports which have been instrumental in ensuring that critical infrastructure is both protected and resilient. She explained that the NIAC and the studies that have been produced have taught the nation that progress and evolvment are completed through trusted partnerships.

Ms. Armstrong proceeded to discuss the current NIAC *Information Sharing Study* noting that there is a need to address this topic in a non-Cold-War paradigm. She stated that the Study is timely, considering the evolving threat situation that has transpired in recent years and compliments both the National Suspicious Activity Reporting (SAR) Initiative and the updated Threat Advisory System.

Ms. Armstrong concluded her remarks by stating that she and the entire Department looked forward to the briefing and deliberations on the NIAC *Information Sharing Study*, identifying it as a foundational effort moving forward and applauding the goal of enhancing the public and private sector partnership. She thanked the attendees for their effort and continued support. Acting Chairman

Berkeley thanked Ms. Armstrong for her remarks, support, involvement, and continued partnership. He then recognized Mr. Kamoie for opening comments.

Mr. Kamoie thanked Acting Chairman Berkeley for the opportunity to provide comments. He stated that he was happy to report that the President had appointed five new members to the Council and noted that from their biographies that these individuals were exceptionally qualified. Mr. Kamoie mentioned that on behalf of the President he appreciated the service and commitment that the Council provided and reiterated that the NIAC has established a long history and proven track record of providing useful and actionable recommendations.

Mr. Kamoie stated that the White House is actively working with Deputy Assistant Secretary Armstrong and Ms. Wong on the NIAC recommendations and that he would provide an update to the Council as appropriate. These recommendations, he concluded, are taken seriously by the White House and noted that they all would be given careful review and consideration.

Mr. Kamoie mentioned the criticality of the public and private partnership and reiterated the importance to share information and stressed that an event has not occurred that has impacted only the public or private sector. He stated that the current NIAC *Information Sharing Study* represents the partnership between the public and private sectors and that this endeavor was timely and important.

Mr. Kamoie closed his comments by discussing critical issues before the National Security Council. He noted in particular potential threats facing critical infrastructure; to include geomagnetic storms. These events could have catastrophic consequences and a great deal of effort has gone into focusing on this issue and potential mitigation. Mr. Kamoie thanked Acting Chairman Berkeley and stated that he looked forward to the deliberations on the NIAC *Information Sharing Study*.

**IV. APPROVAL OF JANUARY 2011
MINUTES**

NIAC Acting Chairman *Alfred R. Berkeley*,
Chairman, Pipeline Trading Systems, LLC
(former Vice-Chairman, The NASDAQ
Stock Market, Inc.)

Acting Chairman Berkeley moved to a discussion of the January 2011 meeting minutes, noting that the Council was not required to formally approve the minutes as after 90 days they become part of the official record. Mr. Berkeley opened the floor for comments on the January 2011 meeting minutes and hearing none moved the meeting to the deliberation of the *Information Sharing Study*.

**V. WORKING GROUP
DELIBERATIONS:
INFORMATION SHARING STUDY**

Alfred R. Berkeley, III,
NIAC Acting Chairman, NIAC
Working Group Co-Chair, Chairman,
Pipeline Trading Systems, LLC
(former Vice-Chairman, The
NASDAQ Stock Market, Inc.)

Michael J. Wallace, NIAC Member,
NIAC Working Group Member,
Former Vice Chairman and COO
Constellation Energy

Acting Chairman Berkeley moved the meeting to a discussion and deliberation of the NIAC *Information Sharing Study*, and introduced himself as Working Group Co-Chair and Mr. Wallace as a Working Group Member.

Mr. Berkeley provided a brief background on the study, noting that it has proven to be one of the largest and most interesting studies that the Council had conducted to date. He stated that the simple phrase of ‘the right information is getting to the right people at the right time’ is a trap and reiterated that this question is one of the most complicated that the NIAC has faced. He then invited Mr. Wallace to begin the presentation on the NIAC *Information Sharing Study*.

Mr. Wallace thanked Mr. Berkeley and applauded his overall leadership of the Study. He noted that this Study represents a compilation of experiences, observations, perspectives, and views on what has and has not worked in the past. Mr. Wallace stated that the Study came at exactly the right time, with 10 years’ worth of experience on these central issues to help better form a partnership between the public and private sector that can lead to actionable steps that produce results for protection and resilience of critical infrastructure.

Mr. Wallace noted that the Working Group Co-Chairs included Mr. Berkeley, Mr. Heasley, and Mr. Nicholson, and that the Working Group members included himself, Mr. Bush, and Mr. Reid. He then proceeded to provide an overview of the Study Group members, noting that they included NIAC members as well as other subject matter experts and executives that brought a wide-span of depth and knowledge on the topic of information sharing. He applauded the group’s efforts and noted that they have worked extremely hard since the study was formally adopted by the Council last October.

Mr. Wallace moved the presentation to a discussion on the background of the study. He reiterated that on April 10, 2010 DHS had requested that the Council conduct an update to a previous NIAC study on intelligence information sharing, and that the request had been adopted at the October 19, 2010 Council Quarterly Business Meeting. He noted that the previous study entitled, *Public-Private Sector Intelligence Coordination*, provided a good foundation for this study to build on, as well as allowed five additional years of experience, observations, perspectives, new regulations, and requirements to be identified and examined. Mr. Wallace stated that the NIAC was tasked to examine three aspects; intelligence information sharing, enhancing owner and operators contributions to counterintelligence, and the role of fusion centers. He noted that with intelligence information sharing the study was addressing the timeliness and relevance of information shared between the public and private sectors and the effect of this bi-directional process. Regarding enhancing owner

and operators contributions to counterintelligence, he advised that the Study had shifted to the examination of counterterrorism and the private sector's role in this process and noted that the private sector was not as familiar with the term 'counterintelligence' but did have experience and understanding of counterterrorism. With fusion centers, Mr. Wallace mentioned that the Study was examining how the private sector can play a more active role in their activity and the challenges that hinder this partnership.

The next topic addressed by Mr. Wallace was the challenge that the Study addresses. He advised that the challenge is achieving a new paradigm of mission-driven, bi-directional information sharing between the Federal Government and the private sector owners and operators of critical infrastructure. To attain this new paradigm, Mr. Wallace stated it would require an adaptive and flexible model much different than the Federal-centric Cold War model which focused on external threats versus internal threats the Nation currently faces. Achievement of this paradigm or model will also require historical competitive issues among entities, in both the Government and private sector, to be identified and removed. Mr. Wallace added that this new model has been slow to develop or gain maturity due to challenges that the Intelligence and Law Enforcement communities have in disseminating sensitive information to a new customer, and prioritizing collection and analysis in new ways. Achieving this model requires the Federal Government and the private sector to spend significant time and resources building trusted partnerships and information sharing processes. Mr. Wallace stated that the value of trusted partnerships cannot be underestimated and the fact remains that individuals in both sectors will come and go, but these relationships need to be fostered to be in a position to deal with potential catastrophes and incidents that the Nation will face.

Mr. Wallace continued the discussion by noting it is imperative to address the challenge of establishing the new model because critical infrastructure is central to the Nation's economic security. The establishment of this new model is a vital element of the Nation's national security and as these critical infrastructure systems become more complex and interdependent, sector vulnerabilities to and consequences from disruptions will continue to increase. Mr. Wallace identified two poignant indicators, noting the 2010 NIAC Study entitled, *A Framework for Establishing Critical Infrastructure Goals*, and the recent events that occurred in Japan at the Fukushima nuclear plant. He elaborated that with the NIAC study, a table-top scenario was created to show the insights and problems that would occur with a catastrophic failure in the Electric Sector and how they would be addressed. From the table-top scenario it was quickly identified that a catastrophic failure would go beyond the ability of the private sector alone to address and that the Federal Government would have to be involved, but did not have the ability, knowledge, experience, or equipment to address the problem. Mr. Wallace also highlighted that the table-top scenario identified that there was no process for the two sides to come together for coordination and interaction. Mr. Wallace stated that the Council's report provides insights in their findings and recommendations that get to the point of the importance of the public and private sector being able to work together if such a catastrophic failure was to occur.

Mr. Wallace concluded his presentation by stating that the public and private sector working together more effectively and efficiently in preparation for a response to a catastrophic incident will be a hallmark finding from the Council's efforts. He thanked Mr. Berkeley and turned the presentation on the NIAC *Information Sharing Study* over to him to continue.

Mr. Berkeley thanked Mr. Wallace and advised the meeting participants that Study was building on prior NIAC work and that as a practice; the Council would rather build on things that already exist rather than reinvent new policies or practices. He continued by stating that, more importantly, the Council likes to build on Federal programs, approaches, and policies of laws that already exist to avoid requesting that new structures be established. Mr. Berkeley further elaborated that building on these approaches provides the opportunity for success and the ability to accomplish goals and reiterated that the study built upon the 2006 NIAC study entitled, *Public-Private Sector Intelligence Coordination* and the 2008 study entitled, *Critical Infrastructure Partnership Strategic Assessment*.

Mr. Berkeley continued the presentation by noting that there is a belief that tension exists between centralization of information and decentralization, and noted that the issue of having centralized command and chain of authority does not seem to work well. He further stated that there needs to be a balance between centralized command and control approaches and distributed approaches that provide imminent knowledge of a particular sector. He concluded that this is not an easy process, but the Council would be looking to have smart individuals with good intentions and judgment address the current circumstances rather than believing that any document or product will anticipate all the potential issues that could arise.

The Study approach was the next topic presented by Mr. Berkeley and he noted that it examines the different stages of information gathering including generating requirements, information collection, analysis and dissemination. He elaborated that different sectors are in different stages of maturity regarding their interacting with the Federal Government. Within the Commercial Facilities Sector, Mr. Berkeley noted that the Real Estate Subsector was one of the hardest entities to understand. It is an industry that is substantially distributed and how it interacts with various sectors of State, local, and Federal Government is an important question to address. He identified a classic problem; an incident occurs in a building and law enforcement or intelligence agencies contact the company that is housed there, not recognizing that it is a tenant who does not own the building. Others, like the Financial Services Sector, view some aspects of their business as highly competitive but do not, for example, see cyber security as a competitive issue and are willing to work together and coordinate. Mr. Berkeley stated these examples were mentioned to impress upon individuals that there is a need to have a sector specific understanding and that individuals on the Federal, State, and local level have to understand and be aware of the detailed knowledge of individual sectors.

Mr. Berkeley stated that the Study examined five sectors in detail and noted that it was not efficient or realistic to review all 18 identified critical infrastructure sectors. He identified the five sectors being examined as Banking and Finance, Chemical, Commercial Facilities, Energy (Oil and Natural Gas), and Public Health and Healthcare and noted that these examinations have identified sector-specific characteristics and approaches to information sharing, and that this information is being synthesized and assessed to identify common characteristics, trends, and gaps in information sharing. To date, he stated that the Study had conducted more than 125 interviews and the work done has been more detailed work than has ever been done before for a NIAC study. In addition to subject matter expert interviews, an examination of open source material has also occurred to include academic and business literature, and other practical approaches. Mr. Berkeley mentioned that there is a belief that there is a tremendous amount of open-source material and that it does not need to be classified and this can assist the Government in its interaction with the private sector.

Authorities and information sharing strategies were the next topic that Mr. Berkeley presented to the Council. He recognized that a number of individuals had provided assistance for this part of the Study and concluded that at this preliminary stage that there was a belief that the Government had all the authorities necessary, but that there appeared to be confusing and duplicative ones that would probably require recommendations on sorting out. Mr. Berkeley stated that there was good reason to have more than one set of authorities and noted that each comes from their own historical background and legislation and this could not be overlooked in the examination. Mr. Berkeley reiterated that the Study attempted to build on programs that were already in existence and identified that the National Infrastructure Protection Plan (NIPP) was viewed as a viable, sensible approach to balancing the sector specific approach with centralization. He also stated that the Study was examining whether the National Information Sharing Environment is relevant and part of any solution and concluded that it might allow for building on existing mechanisms already in place.

Building on these current tools, Mr. Berkeley advised that current structures can serve as blocks for maturing the critical infrastructure sharing processes and that there appeared to be a framework that was being developed in the critical infrastructure information sharing environment. He noted that the Study was still in the information gathering stage but a framework of thought had emerged that focuses on policy or legal authorities, governance, processes in existence, and technology, and is it a repeatable process that is more formalized and mature and working to improve itself. Mr. Berkeley mentioned that the Capabilities Maturity Model at Carnegie Mellon and the software industry, at the request of the Air Force, had developed a model that has the potential to be helpful for framing the Study recommendations.

Mr. Berkeley further elaborated on the interviews conducted for the Study and stated that it was important to reach out to a diverse group of individuals to gather as many perspectives and insights as possible. Instead of interviewing individuals that have their own agendas, Mr. Berkeley stated that the Study had attempted to gain insight from individuals who are involved and execute these issues on a daily basis, in addition to the executives that can carry the message to a higher level and respond at a policy and regulatory level.

Mr. Berkeley stated that an initial finding of the Study was that there are many ways that individuals gather, obtain, and receive information from the Federal Government. He identified that one powerful theme found was existence of previously established relationships which can be utilized to gather and share information. This trusted relationship allows individuals to quickly and efficiently obtain information. Mr. Berkeley noted that the Study would potentially include a recommendation that this type of relationship and its human nature response is something that should not be undone and if it was, the formal channel of communication would have to provide a better value proposition than the information channel of previous relationships.

Mr. Berkeley continued by stating the Study was identifying multiple paths and the process would be the right answer for the next 10 years. He advised that he chose that timeframe because it has been 10 years since the September 11, 2001 attacks and there is recognition that maturity takes time. Established and trusted relationships from agencies and other entities have been in existence for many years and a goal of the Study was to establish a balance between the value proposition in the formal channels of communication and the informal channels. Mr. Berkeley further elaborated that, with formal communications, one finding is there is not enough frequency for informative classified briefings, and he noted that this kind of intelligence does not happen on a regular basis. There is also

a need to examine how individuals communicate formally on an All Hazards basis, so that there is enough interaction and discussion on storms, earthquakes, fires, and natural gas pipeline issues. He concluded that these meetings and interactions would build trust prior to an incident, even if it is not related to terrorism.

The presentation moved to a discussion on general observations for Federal and private sector partners. Mr. Berkeley advised the meeting participants that the term ‘partners’ was carefully selected because, if either side does not view information sharing as a partnership the potential recommendations offered by the Council will not work. One observation made was the public and private sector both realize that there is much to be gained from establishing a partnership which was seen as a distinct change from the past. Mr. Berkeley stated that the way a public agency proceeds on sharing information has a critical influence on whether sharing with the private sector occurs, and he identified the Chemical Sector as a good example of an industry that has made the partnership with the public sector work. He also highlighted examples where a Federal agency has either turned information over to a regulator, which has substantially raised costs for the industry, or publicly made a comment that has hurt an industry’s revenues. Mr. Berkeley advised that he would not mention specifically or identify the negative examples by name, but he was comfortable identifying Chemical Sector because he believed it was a positive example. He summarized that, in the final report, the Council would be more pointed with their recommendations and noted that some Federal initiatives were mature as compared to the Carnegie Mellon Maturity Model that he discussed earlier in the presentation and that some of the initiatives were not.

Mr. Berkeley moved to a discussion of general observations from the private sector and stated that they understand their relationship with their Federal partners is important and continues to evolve. He added that the private sector understands that there is a difference between the Sector Specific Agency (SSA) designated to assist them and a regulating body, and that there is a need to be sensitive about these separate roles. Mr. Berkeley noted the private sector has more work ahead to make the two-way partnership work and to ensure the mechanisms established are truly representative of the industries found within their sectors. He continued by stating that the Study was examining but struggling with various metrics on how to measure effectiveness.

Initial findings for the Federal partners was the next topic covered and Mr. Berkeley mentioned that it was increasingly important that all Federal agencies understand the private sector does have the authority as a legitimate customer of intelligence. He noted the private sector is also a legitimate contributor of intelligence, and identified Suspicious Activity Reports as the Government recognizing the private sector as a legitimate and rightful contributor and stated that there are good examples where the private sector through this reporting mechanism, has provided information which has resulted in prevention of serious incidents. The private sector contribution adds to the value model and allows them to complement the public sector. Mr. Berkeley further elaborated that the SSAs, while varying extensively in their capability, staffing, and maturity, are a critical entity in effective information sharing with the private sector.

Mr. Berkeley next moved to a discussion on predictive analytics and noted that the Study had visited with and interviewed the Virginia State Fusion Center. During this visit, Study participants asked representatives at the fusion center about what contributions from the Federal Government are useful and they responded with a number of valuable examples but were most enthusiastic about an experiment where they had tools conducting in-depth data mining that predicted problems, and

allowed for intervention before the situation or potential threat matured. He concluded that the new computer science tool, called predictive analytics, is a mechanism that the Council would make recommendations on and because most entities will not have the technical knowledge to conduct sophisticated data mining, that there would potentially be a legitimate community role for the Federal Government to further develop this technology and disseminate it out to its private sector partners.

Mr. Berkeley discussed the complexity of engagement points and intelligence information sharing mechanisms with the Federal Government and their tendency to overlap which might be confusing to the private sector. Mr. Berkeley noted the right answer might not be to eliminate the redundancy or overlap, but to explain to the private sector what different individuals and entities are doing and why they are operating the way they are, providing a roadmap for why duplication exists. Regarding the shift in focus from counterintelligence to counterterrorism, Mr. Berkeley stated that counterintelligence was a “loaded” word with specific meaning in the Intelligence Community and that the term ‘counterterrorism’ is more familiar to the private sector. He concluded that the private sector believes that it can provide a unique, value added role in providing counterterrorism information to the public sector.

Mr. Berkeley shifted to a discussion on Government feedback and highlighted that many individuals interviewed for the Study had reported that, when they provided information to the public sector, they often did not receive any response. He further identified that the private sector was interested in receiving feedback on whether or not the information disseminated was useful, or if the information which was sent could be improved to provide more benefit to the public sector. Mr. Berkeley stated that a response back to the private sector, even if to deliver notice of receipt, would assist in providing additional incentive to the private sector in the future and that not receiving a response or feedback would deter them from providing information.

Initial findings for fusion centers were the next topic discussed and it was noted that this mechanism appears to be effective for the Federal Government to leverage its outreach to the law enforcement, first responders, and State and local government communities. He further elaborated that many States have sunshine laws in existence that provide obstacles to the sharing of information with the private sector. For States where there will be no private sector involvement in the fusion centers, DHS needs to establish or find other mechanisms to use for sharing of information. Mr. Berkeley again concluded that this is a question of judgment, authority, and responsibility where decisions will have to be made as to how to get individuals critical information. Mr. Berkeley then turned the presentation over to Mr. Wallace for his final points and comments.

Mr. Wallace thanked Mr. Berkeley and discussed the next steps for the Study. He identified that follow-up interviews and other investigative engagements needed to be completed to clarify, as needed, the understanding of specific intelligence information sharing processes and their effectiveness. He further explained that the next steps also included the development of Study-wide potential recommendations that would be focused on four key structural areas, to include: are the appropriate laws, policies, regulations, and authorities in place to clearly define Federal intelligence-information sharing responsibilities with private sector critical infrastructure owners and operators; what actions must be implemented to ensure Federal intelligence products are aligned private sector risk-management processes, including sector-defined requirements; what actions must be taken to ensure the Federal Intelligence Community and the private sector understand and complement each other’s intelligence capabilities to mutual benefit; and what improvements can be made in the bi-

directional processes that enable the timely sharing of data and analyzed information between the Federal Intelligence Community and the private sector. Mr. Wallace concluded the presentation by stating that he and Mr. Berkeley would be happy to answer any specific questions.

Prior to questions, Mr. Berkeley recognized Ms. Robin Holliday and Ms. Joan Gehrke and identified them as the Study Group Co-Chairs for the *Information Sharing Study*. Mr. Berkeley stated the group had conducted weekly calls since the beginning of the year and he appreciated their great work throughout the process.

Mr. Kamoie thanked Mr. Berkeley and Mr. Wallace for their presentation. He acknowledged that the Study was an impressive piece of work and that the amount of depth of interviews alone certainly contributed to the tremendous insight that had been provided. He recognized that conducting an examination of all 18 sectors would have presented an enormous challenge but asked why the five sectors in the study were selected. Mr. Berkeley stated that the decision was a trade-off between sectors with a variety of differing characteristics, and noted the Commercial Facilities Sector was selected due to the enormous number of facilities located within it. The Chemical Sector was selected due to the approach they adopted previously to work with and engage with the Federal Government versus being forced into a traditional regulation process. Mr. Berkeley stated the Banking and Finance Sector was identified due to subject matter expertise that was available and the sector had experience dealing with cyber, as well as physical issues and the best practices established on how to communicate and cooperate in the sector with cyber issues could assist other sectors in physical security. He concluded that cyber security response might provide some best practices for physical security.

Deputy Assistant Secretary Armstrong asked Mr. Berkeley if cyber issues were kept separate or did the Study take a convergence approach on the issue to which he responded that a convergence approach was selected and highlighted the Financial Services Sector Coordinating Council (FS-SCC) and the Financial Services Information Sharing and Analysis Center (FS-ISAC). Mr. Berkeley noted that the FS-SCC and FS-ISAC have begun to work together because cyber security is an enormous problem for the sector. Mr. Berkeley mentioned that these two entities have gone to DHS and stated that they wanted to develop a protocol for how to get the right high-level individuals in the sector engaged with the Government at the time when an incident is occurring. The goal is to have high-level judgment brought to bear on the downstream consequences to the industry, identify what information needs to be shared, and discuss if the law enforcement model, which Mr. Berkeley stated has hindered the sector in the past, continues to allow an incident to occur until the perpetrator is identified. Though discussions were ongoing, Mr. Berkeley noted that the sector wanted to move forward to break boundaries and engage in the process as much as possible.

Mr. Kamoie offered an additional observation and noted that the decision the Study made to not limit or stop the informal flows of communication and networks was a wise decision. He noted that it would not be wise to attempt to prevent individuals from communicating with one another who had pre-existing relationships and advised that these provided a benefit, though they can be frustrating because they circumvent official processes which would undercut information sharing as a whole. Mr. Kamoie concluded by again thanking Mr. Berkeley and Mr. Wallace for their presentation and noted that he looked forward to the final report later this year.

General Edmonds asked Mr. Berkeley if information was found during the process that would be beneficial if shared. Mr. Berkeley noted that there is a tremendous amount of information that is held routinely and it was identified as a normal course for some companies, but elaborated that on some occasions, this information is shared with peers without thought to share with the public sector. He continued by stating that there have been examples where a number of sectors have established mechanisms to share with each other before sharing with the public sector because there is a fear that the Government will instruct them to stop. He concluded by stating that there are now a number of companies in existence solely to share information among companies prior to sharing with the public sector and this network was substantial. Mr. Wallace added that positive feedback reinforces a desired behavior and reiterated the topic of feedback to meeting participants.

Mr. Berkeley continued his response and stated that there are different maturity levels of the sectors on the private side as well as different maturities of the SSAs, but stated that there was a belief that these were the right model. He stated that some SSAs, to include the Department of Treasury and Department of Energy are not located with DHS and that some located in the Department are found in different offices. Mr. Berkeley advised that this information results in three layers of involvement, budget, mission, and importance in evaluation, and the Study was taking the view that these are evolutionary processes and that smart individuals with good judgment needed to get involved in the process for these to mature and evolve.

Dr. Scott stated that she found the presentation refreshing and pragmatic with a large amount of common sense applied and noted that the concept of an All Hazards examination and building trusted relationships prior to an incident was the correct practice. She concluded that she was impressed with the Study and the recognition of the complexity of relationships, not just public to private, but between businesses was imperative.

Mr. Kepler applauded the work done but advised that he wanted to make a couple of additional points. He mentioned that, if individuals have gone through an incident, they start to develop a relationship with the law enforcement or other Federal agencies involved and suggested that experience is gained. He suggested the idea of having more intelligence briefings where settings can be created so individuals get to familiarize themselves with their partners prior to an incident. Mr. Kepler also stated that there are instances where information sharing is limited by regulation and there needs to be work conducted on a model where information can be shared without violation of laws and regulations.

Mr. Knauss and Dr. Scott suggested that they might have individuals that could bring benefit to the study. Mr. Berkeley stated that he would be happy to talk to Mr. Knauss and Dr. Scott on any ideas they might have in mind. Mr. Berkeley acknowledged Mr. Jim Carey and Mr. Jack Eisenhower for their support to the Study, concluded the presentation and moved the meeting to the Public Comment section.

VI. PUBLIC COMMENT

Nancy J. Wong, DFO, NIAC, DHS

Acting Chairman Berkeley made note that, although no public comments were received, this part of the meeting would remain part of the final record.

**VII. CLOSING REMARKS AND
ADJOURNMENT**

NIAC Acting Chairman *Alfred R. Berkeley*, Chairman, Pipeline Trading Systems, LLC (former Vice Chairman, The NASDAQ Stock Market, Inc.)

Sue Armstrong, Deputy Assistant Secretary, IP, DHS

Acting Chairman Berkeley asked if any of the representatives from the Government, specifically DHS or the White House, would like to provide closing remarks. Ms. Armstrong thanked individuals for their attendance and expressed deep appreciation and admiration for the work that had been conducted on the *Information Sharing Study*. She stated that she was looking forward to the final report and recommendations so that the Department could begin the implementation process. Ms. Armstrong identified that it was a multifaceted mission to protect and make the Nation's infrastructure more resilient and that she appreciated the emphasis on the complexity of the issues that were being recognized in the Study. She further added that the specific questions of authority, competitive interests, and economic vitality in the Study's examination framed a complex problem that has been in existence for a number of years and noted that its observations were groundbreaking. She concluded by stating that the Study is a prime example of building on what has been learned in the past to tackle issues, change expectations and behaviors and she thanked all individuals for attending the meeting.

Acting Chairman Berkeley thanked Ms. Armstrong for her comments, support, and active interaction with the Council. He stated he was proud of the substantial progress that the Council has achieved over the years and stressed the need for cooperation between Government and private infrastructure. Mr. Berkeley again thanked all in attendance and adjourned the meeting.

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

By: *Alfred R. Berkeley* Date: *Dec 27 2011*
Alfred R. Berkeley, Acting Chairman, NIAC

National Infrastructure Advisory Council (NIAC)



Intelligence Information Sharing Study: Working Group Status Update to the Full Council

July 12, 2011

Al Berkeley
Chairman,
Pipeline Trading Systems LLC

Philip G. Heasley
President and Chief
Executive Officer,
ACI Worldwide

James B. Nicholson
President and CEO,
PVS Chemicals, Inc.

Overview

- Study Leadership
- Background
- Tasking to the NIAC: Three Aspects
- The Challenge this Study Addresses
- Study Approach
- Authorities and Information Sharing Strategies
- Building on Current Tools
- Progress to Date
- General Observations
- Initial Findings
- Next Steps
- Questions?

Study Leadership

- Working Group Co-Chairs:
 - **Al Berkeley**, Chairman, Pipeline Trading Systems
 - **Phil Heasley**, President & CEO, ACI Worldwide
 - **Jim Nicholson**, President & CEO, PVS Chemicals

- Working Group Members:
 - **Wes Bush**, President & COO, Northrop Grumman
 - **Jim Reid**, President, CB Richard Ellis Eastern Division
 - **Mike Wallace**, Former Vice Chairman & COO, Constellation Energy

Study Leadership (Study Group Members)

- **Joan Gehrke**, PVS Chemicals, Inc. **(Co-Chair)**
- **Robin Holliday**, Johns Hopkins University Applied Physics Laboratory **(Co-Chair)**
- **Gerald Buckwalter**, Northrop Grumman
- **Ed Goetz**, Constellation Energy
- **Bill Muston**, Oncor Electric Deliver Company LLC.
- **Stanley Szemborski**, Northrop Grumman
- **Dr. Tony DeSimone**, Johns Hopkins University Applied Physics Laboratory
- **Joseph Donovan**, Beacon Capital Partners, LLC.
- **Dr. John Gannon**, BAE Systems
- **Ronald Hicks**, Anadarko Petroleum Corporation
- **Nitin Natarajan**, HHS/ASPR/OPEO
- **Dr. Erin Mullen**, PhRMA
- **Tim Scott**, Dow Chemical
- **Jim Rosenbluth**, Cushman & Wakefield, Inc.
- **Jay Montgomery**, Kinder Morgan
- **Raymond Reese**, Colonial Pipeline

Background

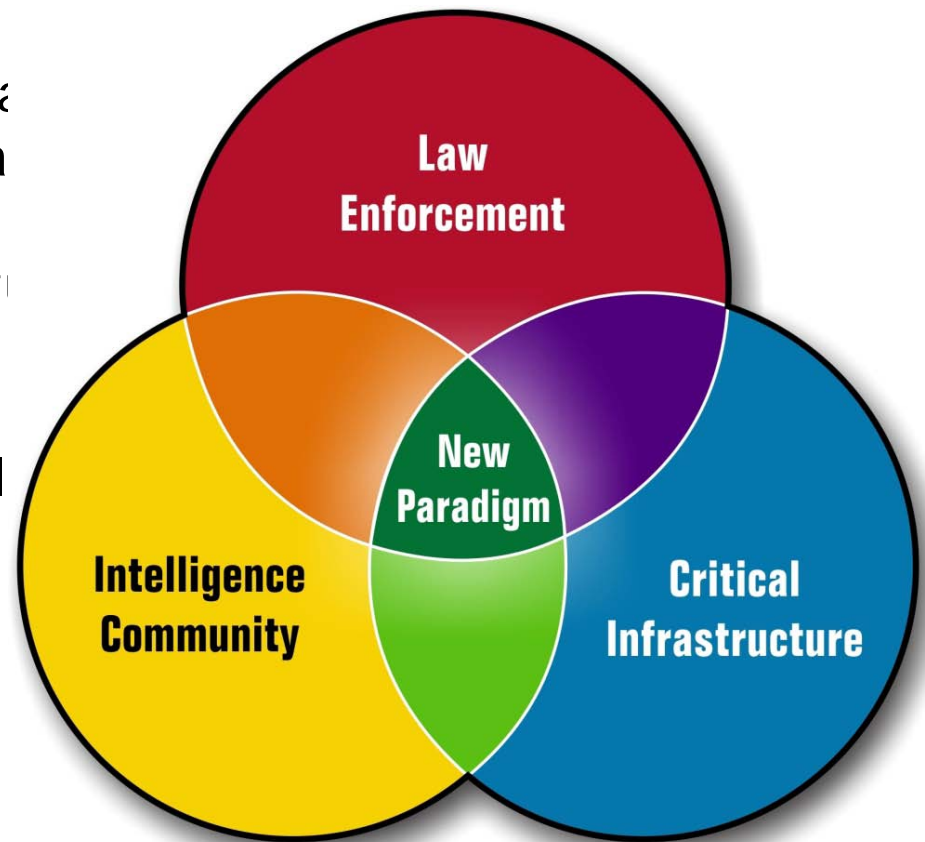
- At the April 13, 2010 NIAC Quarterly Business Meeting, the Department of Homeland Security (DHS) requested that the Council conduct an updated study on intelligence information sharing.
- DHS requested that this proposed study include an examination of the previous findings and recommendations from the 2006 NIAC *Report on Public-Private Sector Intelligence Coordination* as well as the review of new policies and programs, including fusion centers.
- The NIAC approved the study approach at the October 19, 2010 Quarterly Business Meeting.

Tasking to the NIAC: Three Aspects

1. Intelligence information sharing, addressing:
 - The timeliness and relevance of information and intelligence shared between the public and private sectors.
 - The effectiveness of bi-directional processes and products for sharing between government and the private sector.
2. Enhancing owner and operator contributions to counterintelligence, addressing:
 - The private sector role in counterintelligence.
 - Challenges and potential solutions to improving contributions by owners and operators.
3. The role of fusion centers, addressing:
 - Private sector participation and interaction.
 - Information sharing challenges, gaps, and best practices.

The Challenge this Study Addresses

- Mission-driven, bi-directional intelligence information sharing between the Federal government and infrastructure owners/operators is a new paradigm that requires an adaptive and flexible model much different than the Federal-centric, cold-war model still common in the intelligence community.



The Challenge this Study Addresses

- This new model has been slow to develop and mature because it inherently:
 - Challenges the Intelligence and Law Enforcement Communities to disseminate sensitive information to a new customer and to prioritize collection and analysis in new ways.
 - Requires the Federal government and the private sector to spend significant time and resources building trusted partnerships and information sharing processes.
- Addressing this challenge is imperative:
 - Critical infrastructure is central to the Nation's economic security, which itself is a vital element of the Nation's national security.
 - As critical infrastructure systems become more complex and interdependent, sector vulnerabilities to-and consequences from- disruptions will continue to increase.

Study Approach: Build on Prior NIAC Work

- 2006 NIAC *Report on Public-Private Sector Intelligence Coordination*:
 - Strongly supports need for sector-specific frameworks for information sharing.
 - Recommends the development of bi-directional, sector-specific processes for sharing intelligence information with private sector.
- 2008 *Critical Infrastructure Partnership Assessment*:
 - Recommends the ability for sectors to articulate a variety of sector needs, identify sector priorities, and implement strategies.

Study Approach: Information Content and Sources

- Study examines the different stages of information sharing including requirements generation, information gathering, analysis and dissemination.
- The perspectives of chief executives and subject matter experts in business and government are providing the primary sources of information.
 - These engagements will provide the basis for the study findings and proposed recommendations.
- Additional information is being obtained from a comprehensive examination of open source material.

Study Approach: Sector Case Studies

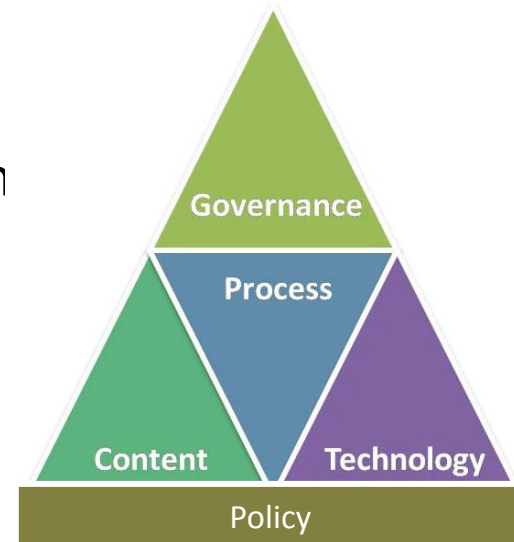
- Five sectors have been selected for in-depth case studies:
 - Commercial Facilities, Healthcare and Public Health, Oil and Natural Gas Segment of the Energy Sector, Banking and Financial Services, and Chemical.
- The case-study examinations:
 - Identify sector-specific characteristics and approaches to intelligence sharing.
 - Illustrate examples of bi-directional information sharing successes and areas in need of improvement.
 - Provide sector-specific observations and findings.
- Case-study information is being synthesized and assessed to:
 - Identify common characteristics, trends, and gaps in intelligence information sharing.
 - Inform study-wide findings and potential recommendations.

Critical Infrastructure: Authorities and Information-Sharing Strategies

- Various legislative authorities guiding intelligence information sharing include the Homeland Security Act and the Intelligence Reform and Terrorism Prevention Act
- National Infrastructure Protection Plan:
 - Unifying National program guiding critical infrastructure protection and resilience efforts.
- National Information Sharing Strategy – articulates the guiding principles for the National Information Sharing Environment (ISE):
 - National ISE Program Manager, Office of the Director of National Intelligence (ODNI), designated the DHS Office of Infrastructure Protection as the Executive Agent for integrating the CIKR private sector as users into the ISE through the CIKR ISE.
 - The Critical Infrastructure and Key Resources (CIKR) ISE and other elements of the National ISE, such as Fusion Centers, likely are key parts of any solution.

Building on Current Tools

- There are current structures and processes that can be building blocks for maturing critical information sharing processes
- For example, the CIKR ISE is a useful construct to guide the maturity of information sharing processes against five elements:
 - Policy – legal authorities
 - Governance – roles, responsibilities
 - Process – capabilities that define info sharing
 - Technology – platforms that enable sector communication and coordination.
 - Content – formalized process that defines information that is required, generated, and received by sector members and other stakeholders.



Progress to Date

- Over 125 interviews, briefings, and executive roundtables have been conducted, involving:
 - Chief executives and private sector owners/operators.
 - Subject matter experts.
 - Federal agency representatives, including the intelligence community.
 - Critical Infrastructure Partnership Advisory Council sector council members.
- Multiple patterns of intelligence sharing have been identified across the five case-studies.
 - Reflects the diversity of business models, risk-management practices, and varying degrees of maturity in the evolving model of bi-directional sharing.
 - Role of all hazards information sharing.
- Study-wide general observations and initial findings have been developed.

General Observations: Federal Partner

Mission	<ul style="list-style-type: none">▪ Intelligence information flow from the Federal government to the private sector is vital to the security and resilience of critical infrastructure.<ul style="list-style-type: none">▪ Most government agencies accept the new paradigm of sharing intelligence information with the private sector, but a culture change is difficult.▪ The mission of a Federal organization has a critical effect on intelligence information sharing.<ul style="list-style-type: none">▪ The Federal Intelligence Community serves multiple customers with widely disparate missions, including diplomacy, law enforcement, military force protection, homeland security and critical infrastructure protection – and information priorities must be balanced among these missions.
Maturity	<ul style="list-style-type: none">▪ Bi-directional flow between the Federal government and the private sector is an <i>evolving</i> model, with widely varying degrees of engagement and implementation by DHS and the various Sector Specific Agencies (SSAs).▪ Continued improvements in information sharing structures and processes are essential and must be implemented through personnel having appropriate judgment and expertise.▪ Overall, effective intelligence information flow remains at an early stage of maturity.
Effectiveness	<ul style="list-style-type: none">▪ While intelligence information sharing has improved since 2006, there are many areas in which major improvements are still needed.<ul style="list-style-type: none">▪ Many CIKR sectors believe that the government does not understand what their critical infrastructure protection information requirements are, and current government intelligence products are of limited value.▪ Multiple redundant government sources of intelligence information create confusion and dilute the impact.▪ Effective bi-directional sharing requires a government feedback mechanism.▪ Linking the right people with the right information at the right time is a paradigm that involves new requirements and complex relationships and will take time to develop.

General Observations: Private Sector Partner

Mission	<ul style="list-style-type: none">▪ Information flow from the private sector to the Federal government is also vital to the security and resilience of critical infrastructure.<ul style="list-style-type: none">▪ By and large, the private sector understands this and is willing to share its information with the government.
Maturity	<ul style="list-style-type: none">▪ This is an <i>evolving</i> model, with widely varying degrees of understanding and engagement among the various sectors.▪ Trusted, personal relationships are used extensively by the private sector.<ul style="list-style-type: none">▪ Relationships are time tested and will remain an important part of intelligence information sharing.▪ These should not replace improved structures and processes designed for the private sector community as a whole.▪ The experiences of sectors in sharing with the Federal government are often quite different.<ul style="list-style-type: none">▪ This reflects the nature of differing sector assets (physical and cyber, open and closed facilities), business models, risk-management, and history of collaboration.
Effectiveness	<ul style="list-style-type: none">▪ Intelligence information sharing has improved since 2006, but improvements are still needed.<ul style="list-style-type: none">▪ The flow of information from the private sector to the government is substantial and growing.▪ It is not clear that the government values information provided by the private sector or is able to act on it in a timely manner.▪ Linking the right people with the right information at the right time requires some refocusing of existing law, structures, staff, training and/or incentives for many sectors to realize systemic improvement – and will take time to develop.

Initial Findings: Federal Partner

- Federal law and policy clearly includes the private sector as a customer of the Federal intelligence community.
- DHS has the clear authority to coordinate the sharing of homeland security information between the Federal government and the private sector.
- Implementation of this authority reflects an early stage of maturity of an evolving model for information sharing.
 - Translating this paradigm into effective practice is a significant challenge to the Federal government, where the practices necessary to ensure *operational* success appear to either not be in place or not well developed.
 - Diverse sector operations require multiple credible flows/channels of information delivery.

Initial Findings: Federal Partner (con't)

- Federal processes and resources are not yet at a sufficient level of maturity to:
 - Adequately reflect the private sector critical infrastructure protection information needs in the Intelligence Community's collection requirements generation process. This leads to major shortcomings in the relevance of intelligence products disseminated to the private sector.
 - Effectively engage 18 critical infrastructure sectors in determining critical infrastructure needs for intelligence information.
 - Implement operational processes for rapid, targeted dissemination of intelligence information.
 - Serve as an effective advocate for critical infrastructure intelligence needs within the Federal intelligence community.
- Sector Specific Agencies (SSAs) vary significantly in the extent and effectiveness of the role as a bridge between an individual sector and the Federal intelligence community.

Initial Findings: Private-Sector Partner

- The private sector generally does not receive the intelligence information they need, though this varies somewhat across sectors.
 - With the exception of asset-specific threats, the majority of information received is reactive to events rather than usefully proactive.
- Predictive analysis (i.e. predictive analytics) is needed so that responsible parties may be proactive in protecting critical infrastructure.
- The majority of information received through formal mechanisms does not meet owner/operator needs.
 - Instances of aligning the right people, time, and information are in the minority of engagements.
- The private sector more readily embraces the bi-directional model.
 - Unlike the Federal intelligence community, the private sector does not have multiple mission areas or the legacy of the traditional model.

Initial Findings:

Private-Sector Partner (continued)

- Engagement points and intelligence information-sharing mechanisms with the Federal government are complex, confusing, and may be redundant and conflicting.
 - As a result, engagement through trusted relationships remains a primary means of facilitating the flow of needed intelligence information.
- Similar to SSAs, the extent and effectiveness of private sector engagement with Federal government partners varies significantly.
 - There are emerging models of success in bi-directional sharing.
 - These models may differ substantially depending upon the nature of sector assets, interdependency, business models, risk-management processes, and relationships.

Initial Findings: Counterterrorism

- Counterterrorism vs. counterintelligence as the practical focus of the private sector.
 - This study found that the term "counterintelligence" has specialized meaning in the intelligence community that is mainly outside of the role of the private sector.
 - This study also found that the term "counterterrorism" is a more accurate term for what the private sector is attuned to and to which it can contribute.
 - Accordingly, the study will use the term "counterterrorism" going forward.
- The private sector believes it has a unique, value-added role in providing this type of information.

Initial Findings:

Counterterrorism (Continued)

- In most cases, the private sector is willing and able to provide such information.
 - This requires trust that the information is valued and acted upon.
- Government feedback is critical to encourage and direct this information flow.
 - Was the information viewed as useful?
 - Was it in fact used?
 - What was the outcome?
 - How can private-sector input be improved?

Initial Findings: Fusion Centers

- The fusion-center mechanism appears to be effective for the law enforcement and first-responder engagement with State, regional, and local communities consistent with its primary mission.
- The use of fusion centers for sharing with the private sector varies widely across locations and sectors, but overall seems comparatively modest.
 - There are, however, several good models of success in this regard.
- As a *mechanism for leveraging resources* across partners, the fusion center appears to be a highly effective model.
- The absence of critical infrastructure protection as a key mission, as well as State laws that govern information protection, appear to be current constraints.
- Fusion centers are likely one of several mechanisms that may address critical infrastructure needs, recognizing that both *needs and resources* vary according to location.

Next Steps

- Complete follow-up interviews and other investigative engagements to clarify, as needed, the understanding of specific intelligence information-sharing processes and their effectiveness.
- Develop study-wide set of potential actionable recommendations, focused on four key structural areas:
 1. Are the appropriate laws, policies, regulations, and authorities in place to clearly define Federal intelligence-information sharing responsibilities with the private sector critical infrastructure owners and operators, and is there any confusion, redundancy, or conflict among these for the multiple federal agencies with intelligence information-sharing responsibility?

Next Steps (continued)

- Develop study-wide set of potential actionable recommendations, focused on four key structural areas (continued):
 2. What actions must be implemented to ensure Federal intelligence products are aligned with and timely for private sector risk-management processes, including sector-defined requirements?
 3. What actions must be taken to ensure the Federal intelligence community and the private sector understand and complement each other's intelligence capabilities to mutual benefit?
 4. What improvements can be made in the bi-directional processes that enable the timely sharing of data and analyzed information between the Federal intelligence community and the private sector?

Questions

Questions?