# Published NIAC Information Sharing Recommendations

- January 2012: Intelligence Information Sharing
  - Improve the Implementation and Accountability of Existing Authorities
    - To improve performance and accountability and help mature DHS's role as a member of the Federal Intelligence Community, the NIAC recommends:
      - a. The Office of the Director of National Intelligence (ODNI) assist DHS in developing, modifying, or assessing programs and processes for private-sector information sharing;
      - b. DHS reexamine the effectiveness of its risk management organizational structure, specifically the separation of threat analysis (in the Office of Intelligence and Analysis) from vulnerability and consequence analysis (in the Office of Infrastructure Protection);
      - c. DHS, supported by ODNI, establish core teams of 3-4 intelligence specialists specifically for each sector, and one team focused on cross-sector information issues;
      - d. ODNI aim to reduce ambiguity and simplify engagement points and processes in the rules and relationships for information sharing; and
      - e. The President define the functions (and authority to execute them), expected outcomes, and accountability measures for Sector-Specific Agencies.
  - Improve the Value of Information Products Industry Risk-Management Practices
    - To ensure that the types of intelligence information used for protection and resilience are shared among partners, the NIAC recommends that the Office of the Director of National Intelligence, working jointly with DHS, establish new intelligence dissemination product formats to create tailored and practical products that help owners and operators protect assets and improve business continuity. DHS and its Federal intelligence partners should supplement classified threat briefings with unclassified reports that can be readily and broadly shared.
  - Build Accepted Practices for Timely Information Delivery
    - All Federal mechanisms for sharing intelligence information should be examined with the goal of simplifying pathways, eliminating redundancy, and ensuring consistency of the information delivered. DHS should collaborate with the private sector to 1) identify critical infrastructure intelligence information sharing pathways and 2) establish sector-specific intelligence information sharing protocols with the specific goal of

improving timeliness. DHS and the Sector-Specific Agencies should work with the Sector Coordinating Councils to create formal networks of private-sector chief security officers and site security managers that will be used to facilitate timely, bi-directional public-private intelligence information sharing.

- DHS should guide Homeland Security Information Network – Critical Sectors (HSIN-CS) implementation to achieve three desired outcomes: 1) sectors are better educated that they are the customer and their needs drive system requirements, 2) system implementation is based on and measured by understanding and meeting these user needs, and 3) system architecture takes advantage of state-of-the-art, commercially available tools for threat analysis in order to meet these needs in a timely manner. Appropriate senior-level management leadership and oversight must be provided to keep this goal on track.

- Enhance Fusion Center Capabilities as One Mechanism for Sharing
  - Where appropriate, DHS should guide fusion centers to establish an information sharing function with owners and operators as part of a critical infrastructure protection and resilience mission. We recognize that not all fusion centers align with critical infrastructure assets, or operate under State laws and policy that allow or encourage the integration of critical infrastructure information. Regardless, DHS should support—through funding, personnel, training, technology, and analytic tools—the development of an infrastructure protection and resilience capability that could stand alone or be integrated within fusion centers to facilitate the flow of intelligence information to and from the private sector, while ensuring information protection and addressing privacy concerns.
  - Where this mission alignment with fusion centers does not take place, DHS should instead direct available critical infrastructure protection resources to an alternative approach specifically designed with information sharing with private sector owners and operators as its goal. If a grant process is used for fusion centers, it should specifically require an infrastructure protection mission and a process for sharing with the private sector.

- <u>October 2010: Optimization of Resources for Mitigating Infrastructure Disruptions</u>
  - Improving the understanding of resilient activities across and among infrastructures and communities
    - The DHS Office of Infrastructure Protection (DHS-IP) should lead a national effort to improve the understanding of resilient activities and how they are implemented in support of combined infrastructure and community resilience

        - Such an effort requires the establishment of a widely shared, well-understood description of the elements of infrastructure resilience and how they can contribute to community resilience. As part of a revised NIPP or as a separate supporting document, DHS-IP should develop—in collaboration with critical infrastructure stakeholders both within and outside of government—a common framework to enable infrastructure and community partners to identify, plan, implement, and assess the various resilience activities.
- Enhancing regional and community-level information exchange
    - DHS-IP should take a leadership role in an initiative to enhance regional and community-level information exchange through the increased availability of data, information, tools, and techniques that may bear upon critical infrastructure protection and resilience. The NIAC especially recommends that this information exchange be expedited through the wider use of fusion centers, and that the NIAC should examine how to enhance infrastructure owner/operator participation in, and contributions to, fusion-center effectiveness in community/infrastructure resilience.
        - The ability for non-Federal entities to plan and execute resilience activities is dependent on good information and the tools and techniques to apply this information to good effect. The transfer of lessons learned and proven technology and organizational-approach models from infrastructure collaborations in Federal information sharing can provide a valuable tool kit for community-level improvements in information sharing.
- Expanding the availability of low-cost, scalable tools and techniques
    - DHS-IP should expand the provision of scalable, low-cost tools and techniques for community-level identification and assessment of infrastructure interdependencies.
        - There are many effective tools and techniques that are widely used on a national level to assess interdependencies and their potential impacts. Further development and transfer of infrastructure-based tools for applications such as dependency analysis and cybersecurity assessment could demonstrably increase the ability of communities to establish an improved baseline of infrastructure assets and their relationship to individual communities or groups of communities. Knowledge of these interdependencies can in turn improve the planning for and use of resources by critical infrastructure operators and the local community.

- Enhancing the transfer of expertise and lessons learned from national-level infrastructure planning and analysis to regional and community-level systems
    - DHS-IP should lead a continuing effort to enhance the transfer of expertise and lessons learned from national-level infrastructure planning and analysis to regional and community-level systems.
        - There is a wide range of valuable expertise and knowledge within Federal, State, and local governments that could, if made available in an appropriate format, bolster community understanding of, and planning for, resilience. The NIAC also encourages the individual sectors, acting through their representative Sector Coordinating Councils or other channels, to identify and make available to local communities tools, techniques, and lessons learned that could enhance local and regional resilience. The NIAC especially encourages larger commercial distribution industries to consider how their supply chain expertise might be applicable to the optimization of resources during an emergency.
- Identifying the impact on critical infrastructure services that result from changes in the Threat Condition under the Homeland Security Advisory System
    - DHS-IP should develop a national "playbook" to be used by DHS to clearly identify the impact on critical infrastructure services that result from changes in the Threat Condition under the Homeland Security Advisory System.
        - In its discussions, the NIAC found that, when the national threat level is elevated, the protective measures associated with this change may have unanticipated consequences on the ability of infrastructure providers to deliver needed services at the regional and community level. To help maintain a community's resilience, infrastructure providers need a clear "playbook" of what actions the Federal government is expected to take with a given change in threat level. In turn, such a playbook will enable infrastructure owners and operators to provide both DHS and their customers with an improved picture of the actions industry will take under the various threat levels and more clearly spell out the implications for service delivery. Ideally, the playbook would address national, regional, community, and sector-specific threat-level changes.
- Removing cross-jurisdictional and other impediments to the transportation and use of outside assets during an emergency
    - The NIAC should prepare a follow-up report to the July 2009 Framework for Dealing with Disasters and Related Interdependencies report to determine the implementation status of recommendations to remove cross-

jurisdictional and other impediments to the transportation and use of outside assets during an emergency. It is recommended that this follow-up report also explore the possibility of implementing standard approaches and agreements to alleviate these constraints.

- Although infrastructure operators generally have well-established processes for working with government within their service areas, moving and applying assets from outside the affected jurisdiction(s) often face significant constraints. A consolidated effort of government and infrastructure service providers, working through appropriate public-private sector partnership mechanisms, should focus on (1) identifying key cross-jurisdictional bottlenecks and (2) implementing standard approaches to remove these impediments for the purposes of optimizing the sharing of resources during major disruptions. One example is the development of credential standards needed to respond to all hazards, as directed by the Post Katrina Emergency Management Reform Act of 2006.

- <u>October 2010: A Framework for Establishing Critical Infrastructure Resilience Goals</u>
  - The White House should initiate an executive-level dialogue with electricity and nuclear sector CEOs on the respective roles and responsibilities of the private and public sectors in addressing high-impact infrastructure risks and potential threats, using an established private sector forum for high-level, trusted discussions between industry executives and government leaders.
    - It is critical to create opportunities for public-private partnership using excellent models, like the Critical Infrastructure Partnership Advisory Council (CIPAC), that already exist. While these partnerships typically bring much-needed functional expertise to the table, most of the participating individuals are not empowered to make decisions for other parts of their organization or have the ability to influence sector CEOs on priority issues. What is needed is an executive-level forum of private sector CEOs and their government counterparts to focus on high-level policy issues; create a framework for public-private collaboration with defined roles and responsibilities; and make recommendations that strengthen overall resilience, especially for high-impact, low-frequency risks.
  - The nuclear and electricity industries should each develop an emergency response plan that outlines a coordinated industry-wide response and recovery framework for a major nationwide disaster.
    - Although electric and nuclear utilities have robust emergency response plans and exercise them regularly, there is no industry-wide plan to

address a major national disaster. Although relationships between the companies and their States, regions, and communities are well established, the relationships, roles, and responsibilities at the national level are less clear. The Council recommends that coordination and development of such an emergency response plan be led by CEOs in each sector and aligned with the National Response Framework and National Incident Management Systems. The CEO Business Continuity Task Force of the Electric Edison Institute (EEI) could lead this effort within the electricity sector, in coordination with NERC, the American Public Power Association, and the National Rural Electric Cooperative Association. The Nuclear Energy Institute could lead this effort within the nuclear industry.

- DHS and other Federal agencies should improve information sharing with the private sector by providing focused, actionable, open-source information on infrastructure threats and vulnerabilities
    - While some information can only be shared in a classified setting, many of the useful incidents and trends can be culled from open sources and distilled into actionable recommendations to the private sector. The NIAC heard several examples of executives who gained key insights from analysis of open-source information that was tailored to their sector. DHS and other Sector-Specific Agencies should work with their private sector counterparts through the CIPAC structure to identify the types of information that would be most valuable to owners and operators and the best mechanism to deliver it to them. DHS and other government agencies should develop more effective ways to share classified content with the electricity and nuclear sectors, or translate it into useful non-classified information.
- All critical infrastructure sectors should consider adopting the industry self-governance model exemplified by the Institute of Nuclear Power Operations (INPO) and the North American Transmission Forum (NATF) to enable the private sector to collaborate on industry-wide resilience and security issues outside the regulatory compliance process
    - The nuclear industry created INPO as a private organization to address critical safety and reliability issues in the aftermath of the Three Mile Island disaster. Its defining feature is a self-governing model that commits each company to achieve excellence in nuclear power plant operations. This is backed up by plant evaluations that are shared confidentially within the nuclear sector, outside the regulatory process. More recently, the NATF has adopted this model to address transmission reliability and resilience issues across the electricity sector. These organizations create an opportunity to provide regular evaluations of the resilience and security of

sector assets and systems, establish performance objectives, train and educate sector employees, and create CEO accountability for any shortcomings in performance. The self-monitoring nature of such an organization would not be a substitute for existing regulation, but would provide an extra measure of responsibility and care for overall industry performance.

- Promote the use of the NIAC-developed framework for setting resilience goals in the CIKR sectors and for providing a common way to organize resilience strategies within Federal and State governments and CIKR sectors
    - The goal-setting framework developed by the Council should be used to help critical infrastructure sectors discern their resilience goals. The process enables sectors to not only establish outcome-based goals but also uncover gaps in sector resilience and develop options to address them. The process establishes a baseline of current practices, develops high-level resilience goals, tests the sector's resilience in a high-impact scenario, and addresses gaps and seams through a public-private dialogue. The process is flexible enough to be used by all CIKR sectors despite their differences in assets, businesses, and risk profiles. DHS should consider using this resilience framework as a common way to organize resilience strategies and programs.
- DHS should support modeling and analysis studies of the cross-sector economic impacts of CIKR failures using tools such as input-output analysis
    - Many of the CIKR sectors are highly interconnected, which can improve resilience but also create new opportunities for problems to cascade across sectors, regions, and economic systems. Understanding the impact of sector failures is becoming more important as infrastructures become increasingly interconnected. The NIAC report, Critical Infrastructure Partnership Strategic Assessment, recommended that the government increase resources to conduct cross-sector studies and analyses, guided by private sector knowledge of infrastructure operations. The NIAC reaffirms this recommendation and highlights the need to place special emphasis on supporting studies that apply established economic models and tools to examine how increased interconnection affects infrastructure resilience and economic impacts.
- The Federal government should work with owners and operators to clarify agency roles and responsibilities for cyber security in the electricity sector, including those for cyber emergencies and highly sophisticated threats
    - The Federal regulatory framework and roles for all stakeholders involved in securing the electric grid should be clear to avoid duplicative or conflicting actions in times of crisis. The electric utility industry is not in

the law enforcement or intelligence gathering business, and the government has limited experience operating the electric grid. Thus, each should be consulted, and the flow of information should be regularly exercised, before a threat becomes a crisis. To avoid confusion, those at the highest levels of government and industry should be involved in coordinating responses and declaring the need for emergency action. The electricity industry is also facing new highly sophisticated cyber threats, possibly from nation-states, that may exceed the capability and responsibility of owners and operators. The Council recommends that the White House work with electricity sector CEOs to clarify public and private roles and responsibilities in managing these cyber risks that could compromise the integrity of the bulk power system.

- <u>September 2009: Critical Infrastructure Resilience</u>
    - Fortify government policy framework
        - The government should use a White House level authority to adopt a common definition for resilience and disseminate a high level, top-down strategy for the development and funding of resilience efforts.
    - Improve government coordination
        - Increased coordination among all levels of government and CIKR owners and operators is critical to mitigating the potentially detrimental effects of competing regulations and standards across regions, states, and local entities. The White House should coordinate and adjudicate conflict among regulatory agencies and actions in each sector to support the established resilience goals.
    - Clarify roles and responsibilities of critical infrastructure partners
        - Review current incident management documents including the National Response Framework and National Incident Management System and identify opportunities to expand training and outreach activities to the CIKR owners and operators. Such activities provide Federal, state and local entities a better understanding of the components of resiliency during an event and allow for increased information sharing.
    - Strengthen and leverage public-private partnership
        - Make full use of existing public-partnerships to provide a set of common, agreed upon sector specific goals, with clear input from both CIKR owners and operators and government on feasibility and objectives.
    - Implement government enabling activities & programs in concert with critical infrastructure owners and operators
        - Exercises involving fact-based scenarios are critical to identifying cross-sector interdependencies. Exercises allow CIKR owners and operators to execute their continuity of operations plans and make adjustments where

unforeseen gaps occur. Plans for such activities must include evaluation of critical infrastructure resilience after an event as well as a means for distributing lessons learned to an audience wider than exercise participants.

- July 2009: Framework For Dealing With Disasters and Related Interdependencies
  - A Process for Identifying and Addressing Statutory, Regulatory and Policy Impediments to Recovery
    - DHS should institutionalize processes and provide funding as needed to systematically develop and maintain at the Federal, State and local (especially major metropolitan) government levels, catalogs of laws and regulations that may need to be suspended or modified during disaster scenarios. Similar to an effort undertaken by the City of New York, planners should apply the following four-step process in their disaster preparedness work:
      - Identify relevant disaster scenarios and compile existing response plans for each
      - Determine for each whether the government planned response:
        - Complies with all applicable Federal, State and local laws and regulations, and
        - Could pose any meaningful risk of hindering CIKR/ community recovery or incur liability for the acting government authority
      - Catalog all instances where planned action is not authorized and determine whether the applicable laws or regulations can be modified, suspended, or waived. Draft appropriate emergency orders for use during a disaster
      - For laws or regulations that cannot be modified, suspended, or waived, planners should develop a work-around. Government should seek to identify all legal and regulatory requirements affecting CIKR operators for which no timely legal waiver process presently exists, and take steps to afford waiver.
      - Private Sector CIKR operators should conduct an effort in parallel with these steps as well to identify areas of statutory or regulatory impediment and communicate these to the relevant authority.
  - Potential Federal, State and Local Action to Address Statutory, Regulatory and Policy Impediments to Disaster Recovery/Preparedness
    - Congress should validate the “Alternative Arrangements” rule of the Council on Environmental Quality (CEQ) to address the lengthy waiver process for EIS.

        - The NIAC recommends a list of specific actions to address other statutory, regulatory, and policy impediments which include:
            - A simple process for emergency waivers for document filing deadlines with regulatory agencies
            - A standardized and coordinated approach for processing requests and issuing waivers for regulatory filing requirements for banks during a disaster
    - Improved Private Sector-Government Cooperative Efforts in Disaster Recovery
        - The DHS, Federal Emergency Management Agency (FEMA) and DHS Office of Infrastructure Protection (IP) should collaborate to develop and disseminate best practices for authorities to use in credentialing and granting access to CIKR workers in a disaster area during an emergency. The developed solution should:
            - Leverage recent accomplishments and lessons learned from the Gulf Coast region during hurricanes Gustav and Ike
            - Collaborate the All Hazards Consortium (AHC) and similar, well-positioned organizations
        - DHS-FEMA and DHS-IP should develop reliable best practices for information sharing during disaster recovery operations, including:
            - Inclusion of private sector CIKR operators in EOCs and planning exercises
            - Strong sector-to-sector communication during a disaster
            - Sector information sharing mechanisms, such as the sector Information Sharing and Analysis Centers (ISACs), for sector communications outside the disaster area
            - EOC decision makers establishing and communicating recovery priorities
    - Cooperative Planning for CIKR Emergency Preparedness
        - The DHS-FEMA and DHS-IP should collaborate with regulatory agencies to identify potential disaster scenarios where the lead authority for government response is unclear to private sector CIKR owners and operators and develop a workable response plan.
        - DHS should include the Water Sector in all disaster/emergency response and recovery training and exercises as a best practices approach to planning. Recommendations also outline steps for:
            - Availability of grants for water systems auxiliary backup power systems investments for key Water Systems sites during electrical outages.

        - Elevation of Water Services to an "emergency support function" (ESF) within the National Response Framework (NRF) during the next revision cycle.
        - Inclusion of a Water/Wastewater Agency Response Network (WARN)-focused curriculum in Emergency Management Assistance Compact (EMAC) training programs.
    - DHS-FEMA and DHS-IP should collaborate to develop and disseminate a best practices guide for disaster planning exercises to State and local governments. These best practices should promote inclusion of private sector CIKR operators in planning and executing disaster exercises and scenarios and include the following elements:
        - Regionally-based exercises that emphasize CIKR disaster recovery planning and response.
        - Table top exercises focusing on communication between multiple levels of Government
        - Involvement of CIKR owner-operator participation in all relevant planning for exercises.
        - Clearly established roles and responsibilities for government and private sector CIKR owner operators during major disasters
        - Communication and coordination on CIKR restoration priorities.
        - After-action review of disaster events and exercises to include Federal, State and local governments as well as CIKR owner-operators to identify gaps and lessons learned
        - Validation of emergency plans from smaller CIKR owner-operators
        - Acknowledgement that different governments will have different priorities for restoration of some types of CIKR outages
    - Emergency response authorities should help protect private sector resources from ad hoc commandeering by local officials.
- <u>October 2008: Critical Infrastructure Partnership Strategic Assessment</u>
    - Reaffirm the Critical Infrastructure Protection Mission and the Public-Private Partnership
        - Reaffirm the importance of critical infrastructure protection and resilience as a fundamental mission of government and a responsibility of business
            - The Secretary of Homeland Security should communicate the importance of the critical infrastructure protection and resilience mission to the presidential candidates and their transition teams.
            - The leader of each Sector-Specific Agency should ensure that tailored briefing materials are prepared for the President's transition team and executive appointees covering the status of

their sector's infrastructure protection issues and the role of the public-private partnership.
        - The NIAC should conduct a study to examine what steps government and industry should take to best integrate resilience and protection into a comprehensive risk-management strategy.
        - The NIAC Secretariat should make this study widely available and distribute it to incoming members of Congress and staff, as well as to the leadership of the nation's private sector.
    - Reinforce the partnership as a priority throughout government
        - The Secretary of Homeland Security and the White House should reaffirm the goals, objectives, and vision of the sector partnership.
        - The new President should affirm his commitment to the public-private partnership and make it a priority throughout the government with cabinet-level accountability.
        - DHS and the Sector-Specific Agencies should encourage the Sector Coordinating Councils and the Government Coordinating Councils to develop strong working relationships with appropriate business organizations, and state, local, and regional security partners within the sector partnership.
- Reinforce Key Principles of a Successful Partnership Structure
    - Strengthen senior leadership engagement in and commitment to the partnership in both government and industry
        - The private sector should initiate a strategic dialogue between industry CEOs and the White House soon after the inauguration to reinforce their commitment to partnership principles, followed by similar dialogues with the Congressional leadership and state governors.
        - Owners and operators of each critical infrastructure sector should clarify their value proposition and work with DHS or the Sector-Specific Agency to reinforce it among government security partners.
        - Private industry and government partners should adopt a self-scalable sector engagement model that builds trust among peers at the executive and operational levels
    - Leverage relationships to maximize engagement
        - Each Sector Coordinating Council should develop a partnership map that identifies complementary and interdependent partners who can help strengthen the country's critical infrastructure security.

- DHS or the Sector-Specific Agencies should encourage each Sector Coordinating Council to develop strategies to diversify sector council membership and broaden partnership connections by tapping into established sector organizations

- Update the Sector Partnership Model to Be More Efficient and Effective
  - Increase flexibility in the sector partnership to better accommodate diverse sector needs.
    - DHS should tailor partnership requirements to match individual sector characteristics and partnership development needs
    - The Sector Coordinating Councils and the Partnership for Critical Infrastructure Security should nurture peer assistance and share lessons learned to help all sectors improve their partnership practices.
    - DHS should encourage Sector Coordinating Councils to develop strategic roadmaps to enable sectors to articulate a variety of sector needs, identify sector priorities, and implement protection and resilience strategies.
  - Emphasize cross-sector interdependencies and collaboration through the Sector Partnership Model
    - DHS and other federal organizations should increase resources to conduct cross-sector studies and analysis, guided by private-sector knowledge of infrastructure operations
    - Increase understanding of cross-sector interdependencies and capabilities, led by the sectors that have a well-established partnership and a strong security posture
  - Improve government practices and coordination in strengthening the Sector Partnership Model
    - DHS and federal agencies should reinforce partnership engagement expectations throughout government and create a culture of collaboration that includes incentives, training, and compliance with the Ethics Guidelines
    - DHS and the Sector-Specific Agencies should put processes and practice in place to ensure that owners and operators are engaged in the early stages of developing policies, processes, and documents that may affect them or result in requests for sector information and inputs
  - Streamline government processes and requirements on the Sector Partnership Model and provide adequate resources to comply with them
    - DHS should reexamine its internal reporting requirements, establish realistic response times, clarify expectations of the Sector

Coordinating Councils and the Sector-Specific Agencies, and conduct an analysis of authorities and internal processes to determine how requirements might be streamlined
    - DHS and the private sector should increase the availability of resources, where appropriate, to meet DHS partnership requirements and requests for information
- April 2008: The Insider Threat to Critical Infrastructures
    - Government should create a clearinghouse resource for owner-operators to assist in the assessment and mitigation of their insider threat risks, leveraging the structures in the Education and Awareness recommendation as well as the accompanying Report Appendices.
    - Government should establish a mechanism to communicate intelligence agency understanding on insider threats, making use of cleared personnel in each sector and provide periodic, useful briefings on developments about insider threats
    - Government should develop a mechanism and validated process to share information on national security investigations in order to address a specific information-sharing obstacle identified by the NIAC between government and critical infrastructure owner-operators.
    - Each sector should establish a trusted process and mechanism to share incident information on insider threats in a protected manner. Protected information can be aggregated anonymously to inform CIKR risk assessments in all sectors
- January 2008: Chemical, Biological, and Radiological Events and the Critical Infrastructure Workforce
    - Chemical Event Recommendations
        - Evaluate chemical threats against comprehensive, national assessment priorities, and establish a risk-based prioritization schema for chemical response measures
        - Provide accelerated development, training, and support of local Fusion Centers to enhance robust on-the-ground capabilities. Continue joint training exercises conducted at chemical facilities to enhance and expand knowledge of chemical event responsiveness
        - Improve information sharing and outreach efforts via the Homeland Security Information Network (HSIN) chemical portal
        - Expand the Department of Homeland Security's Chemical Review Program to multiple regions of the country to help reduce duplicative efforts and promote all hazards planning by emergency responders. Expand participation in the program to include other first responders, including local law enforcement.
        - Fully integrate lessons learned into the National Incident Management System (NIMS) and other preparation and response programs

        - Continue to improve operability and interoperability of communications among responders. Consider solutions to propagate communications technologies to those who may potentially engage in a chemical event response, including the private sector
        - Continue to build public/private-sector relationships through the sharing of information and the protection of competitive and sensitive data. Assist the private sector to better identify information needed by governmental agencies
    - Radiological Event Recommendations
        - Develop and deploy training materials for all first responders. Content is readily available and deployable; awareness and distribution could be enabled through directed marketing and communications, inclusion in structured exercises, or other mechanisms already in place
        - Clearly establish, communicate, and reinforce a radiological event focal point, lead agency, chain of command, and protocol for response coordination and communication. Define and make widely known the roles and responsibilities for lead and supporting Federal agencies
        - Leverage industry knowledge, tools, or experience in radiological event planning, preparedness, and response efforts. Establish, in advance, mechanisms to leverage industry resources in radiological events. Employ tools and technologies in place today to further capabilities.
        - Continue to make progress on plans and response programs that assess and prioritize radiological threats and vulnerabilities within the context of other events (e.g., chemical and biological). Improve knowledge around specific scenarios, impact, and likelihood of events. Assess the usability and availability of data; make necessary information available to first responders who will benefit from additional intelligence. Continue to deploy tools to support planning and response scenarios.
    - Biological Event Recommendations
        - Communications-Related Recommendations
            - Pre-define, to the greatest extent possible, a consistent biological event communications plan, complete with tailored communications to specific target audiences based on various possible scenarios
            - Develop and pre-position, to the greatest extent possible, communications in all distribution channels, including radio, television, telephone, print, and online media
            - Continue to engage the private sector to augment the distribution of communications to the critical workforce

        - The public- and private-sector Critical Infrastructure partners should continue refining their existing communications plans, processes, and success metrics through series of response exercises. These exercises should include participation from appropriate state and local representatives where feasible. The Federal government, in consultation with the critical infrastructure owners and operators, should develop a mechanism to refine and identify those priority workforce groups within and across the 17 CI/KR sectors.
    - Dissemination-Related Recommendations
        - All public- and private-sector partners should continue educating their relevant stakeholders on biological plans, processes, and priorities
        - The public and private sectors should align their communications, exercises, investments, and support activities absolutely with both the plan and priorities during a biological event. Continue data gathering, analysis, reporting, and open review.
    - Response and Containment Recommendations
        - Public and private partners should work closely to define more clearly response and containment roles and responsibilities, as well as response timelines and milestones
        - The Federal government must do a better job in educating all stakeholders on plans, processes, and priorities
        - Using this report's findings as a baseline for future work, the Federal government should develop an innovative and easy-to-use mechanism to clearly identify the priority workforce groups
- <u>January 2007: The Prioritization of Critical Infrastructure For A Pandemic Outbreak in the United States</u>
    - Communications-Related Recommendations
        - Pre-define, to the greatest extent possible, a consistent pandemic communications plan, complete with tailored communications to specific target audiences based on various possible pandemic scenarios
        - Develop and pre-position, to the greatest extent possible, communications in all distribution channels, including radio, TV, telephone, print, and online media
        - Continue to engage the private sector to augment the distribution of communications to the critical workforce
        - The public- and private-sector critical infrastructure partners should continue refining their existing communications plans, processes, and success metrics through a series of response exercises. These exercises

should include participation from appropriate state and local representatives when feasible. The Federal government, in consultation with the critical infrastructure owners and operators, should develop a mechanism to refine and identify those priority workforce groups within and across the 17 CI/KR sectors

- Dissemination-Related Recommendations
  - Consider alternative distribution strategies and guidance to give owner-operators a stronger voice in determining which employees receive higher prioritization for vaccines and antiviral medications. Build flexibility into distribution frameworks to allow the private sector to receive, distribute, and, with appropriate medical support, dispense vaccine and antiviral medications to their critical workforce
  - All public- and private-sector partners should continue educating relevant stakeholders on pandemic plans, processes, and priorities
- Preparedness and Communications
  - The public and private sectors should align their communications, exercises, investments, and support activities absolutely with both the plan and priorities during a pandemic influenza event. Continue data gathering, analysis, reporting, and open review
- Surveillance and Detection
  - Developing a formal framework designed to engage international components of U.S. corporations in global bio-data collection efforts
- Response and Containment
  - Public and private partners should work closely to define more clearly response and containment roles and responsibilities, as well as response timelines and milestones
  - The Federal government must do a better job in educating all stakeholders on plans, processes, and priorities
  - Using this report's findings as a baseline for future work, the Federal government should develop an innovative and easy-to-use mechanism to identify the priority workforce groups clearly

- <u>January 2007: Convergence of Physical and Cyber Technologies and Related Security Management Challenges</u>
  - Information Sharing
    - The Council 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
      - DHS enhance the control system cyber incident information collection mechanism at Carnegie Mellon's CERT Coordination

Center (CERT/CC) for comprehensive 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
- 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).
- <u>July 2006: Public-Private Sector Intelligence Coordination</u>
    - Senior Executive Information Sharing
        - Develop a voluntary executive-level information sharing process between critical infrastructure CEOs and senior intelligence officers. Begin with a pilot program of volunteer chief executives of one sector, with the goal of expanding to all sectors
    - Best Practices for the Private Sector
        - The U.S. Attorney General should publish a best practices guide for private sector employers to avoid being in conflict with the law. This guide should clarify legal issues surrounding the apparent conflict between privacy laws and counter terrorism laws involving employees. Moreover, it should clarify the limits of private sector cooperation with the IC
    - Existing Mechanisms
        - Leverage existing information-sharing mechanisms as clearinghouses for information to and from critical infrastructure owners and operators. This takes advantage of the realities that exist sector by sector
    - National-Level Fusion Capability
        - Establish or modify existing government entities to enable national- and state-level intelligence and information fusion capability focused on Critical Infrastructure Protection (CIP).
    - Staffing
        - Create additional “Sector Specialist” positions at the executive and operational levels as applicable in the IC. These specialists should be civil servants who have the ability to develop a deep understanding of their private sector partners
    - Training
        - Develop an ongoing training and career development program for sector specialists within intelligence agencies
    - RFI Process
        - Develop a formal, and objectively manageable, homeland security intelligence and information requirements process, including requests for information (RFIs). This should include specific, bi-directional processes tailored sector by sector.
    - Standardize SBU Markings and Restrictions
        - The Federal government should rationalize and standardize the use of SBU markings, especially “For Official Use Only” (FOUO), and publish standard handling instructions clearly for all intended recipients

- April 2006: Workforce Preparation, Education and Research
  - None applicable
- October 2005: Sector Partnership Model Implementation
  - Validate Conceptual Structure
    - Sector Coordinating Councils (SCCs) and Government Coordinating Councils (GCCs) should comprise the base level of the model
    - There was consensus regarding the second level of the model—the Private Sector and Government Cross-Sector Councils. The Partnership for Critical Infrastructure Protection (PCIS) should assume the role of the Private Cross-Sector Council.
    - PCIS must have a government counterpart, the Government Cross-Sector Council, consisting of the GCC Chairs
    - The Government Cross-Sector Council must engage state Homeland Security Advisors (HSAs) in the model
    - The Office of the Under Secretary of Preparedness should be included to show information flow between that office and both cross-sector councils with no connotation of subordination; any directional arrows must be removed, since they imply subordination
    - DHS should eliminate the top level of the organization (the NIPP Leadership Council), given that its work is redundant
  - Validate Model Composition and Representation
    - DHS should recognize all SCCs equally and should recognize them in the manner in which they have chosen to organize themselves. SCCs should constitute themselves in a way that provides for appropriate governance and representation of the whole sector
    - If DHS or another government agency has a request of an SCC, that agency should coordinate with the Sector Specific Agency, as it is the principal focal point for coordination with that SCC and sector
  - Assess Operational Framework Options
    - The NIAC recommends that the operational framework for the Sector Partnership Model be based on an unconditional exemption pursuant to Section 871 of the Homeland Security Act of 2002. The exemption authorizes the establishment of advisory committees as the Secretary may deem necessary and provides that an advisory committee established under this section can be exempt from FACA.
  - Key Processes and Principles
    - The NIAC identified the following key processes and principles to support a true partnership:
      - Stakeholders develop a true partnership based on a collaboration of equals in which all partners bring value

- SCCs are self-formed entities. The private sector is responsible for group formation, membership, and governance
- The SSA acts as the government lead for coordinating with the sector. All government agencies should recognize the role of the SSA, and use it as their means to interface with the SCCs. Sectors having a DHS office as their SSA will use that DHS office as their government interface
- Government communication to the sectors should occur primarily through the established SCCs, supported as necessary by the councils' designated information sharing and analysis mechanisms. Exceptions do exist, such as when dealing with threat-based information that needs to reach the affected owners and operators as quickly as possible
- All participants in the partnership model must fully engage in the ongoing development, implementation, and improvement of national plans, including the NIPP, SSPs, NRP and the National Incident Management System (NIMS). This encompasses:
    - Sector-wide planning
    - Development of sector best practices
    - Sector-wide dissemination of programs and plans
    - Cross-sector coordination
    - Facilitation of response and recovery
- Given that disasters happen at a regional level rather than a national level, it is important to ensure the model synchronizes activities down to the regional level.
- The Protected Critical Infrastructure Information (PCII) Program and the Homeland Security Information Network for Critical Sectors (HSIN-CS) are tools to facilitate information sharing, given the following:
    - Recognize the concept of "originator control" for all information submitted by the private sector as PCII, which would allow the submitter to limit how the information is used.
    - When requesting information, the government must clarify why it needs the information, and it must explain how it intends to use it.
    - All voluntary private-sector responses to a government data call should be deemed PCII.

        - Legal protections must ensure that information voluntarily submitted as PCII will not be used for existing or additional regulation or government mandates.
        - PCII protection must be extended to CIP information voluntarily submitted by industry to agencies other than DHS; time is of the essence when dealing with threat information.
        - When housed on HSIN-CS, all information provided by the private sector should remain the property of the private sector and thus not be subject to disclosure under FOIA.
        - The HSIN-CS portal should include a clearly delineated, simple mechanism for submitting information as PCII.
    - Other Recommendations
        - Crisis management plans should exist for each sector and be tested. Testing should include validation of cross-sector coordination. Testing and exercising sector crisis management plans should be under the purview of the sector coordinator
        - Establish a command center that provides a call tree, alerting mechanism, and communication point for use by critical sectors during an emergency.
        - DHS should sponsor crisis management exercises that include the participation of the critical infrastructures, as soon as possible, and annually thereafter
        - Provide a framework for public and private emergency management interaction including national sector, state, regional, and local levels. This framework must account for information sharing mechanisms as well as review of significant public/private partnerships
- <u>October 2005: Risk Management Approaches to Protection</u>
    - Overall Recommendation
        - Continue the government's focus on risk management
    - Specific Recommendations
        - Create and standardize risk management methodologies and mechanisms across the government
        - Establish a risk management leadership function within departments, bureaus or agencies
        - Establish risk management oversight function
- <u>October 2004: Common Vulnerability Scoring System</u>
    - Support use of the CVSS by all Federal departments and agencies. Those departments and agencies involved in identifying, reporting, and scoring vulnerabilities should develop Base and Temporal scores to contribute to the worldwide body of knowledge for each vulnerability. All departments and

agencies should compute Environmental (i.e., Final) scores as they become involved in remediating and resolving vulnerabilities.

- Encourage DHS to promote the use of CVSS by the global vulnerability management community, including international, state, local, and tribal governments, critical infrastructure owners and operators, and discoverers, vendors, coordinators, and users
- Coordinate with the NIAC to identify an organization to function as the permanent home for CVSS. This organization should be responsible for maintaining and updating CVSS metrics and formulas. It should also possess significant technical expertise and experience managing vulnerabilities, and should maintain a global focus