U.S. DEPARTMENT OF HOMELAND SECURITY

HOMELAND SECURITY ADVISORY COUNCIL

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE - 13 NATIONAL SECURITY MARITIME STRATEGY:

REPORT ON THE IMPLEMENTATION PLANS FOR MARITIME TRANSPORTATION SECURITY MARITIME COMMERCE SECURITY AND MARITIME INFRASTRUCTURE RECOVERY

APRIL 28, 2005

JOSEPH J. GRANO, JR.
CHAIRMAN
HOMELAND SECURITY ADVISORY COUNCIL

FRANK J. CILLUFFO
CHAIRMAN
TASK FORCE ON HSPD-13

WILLIAM H. WEBSTER
VICE CHAIRMAN
HOMELAND SECURITY ADVISORY COUNCIL

MICHAEL CARONA
VICE CHAIRMAN
TASK FORCE ON HSPD-13

DANIEL J. OSTERGAARD
EXECUTIVE DIRECTOR
HOMELAND SECURITY ADVISORY COUNCIL

CANDACE STOLTZ
DIRECTOR
TASK FORCE ON HSPD-13

TABLE OF CONTENTS

ACKNOWLEDGMENTS

Mr. Cilluffo acknowledges and commends the efforts of the entire Task Force and the support of the staff of the Homeland Security Advisory Council in the production of this report. Mr. Cilluffo expresses particular appreciation to Ms. Candace Stoltz, the Designated Federal Official to the Task Force; LCDR Howard Wright, U.S.C.G, Coast Guard liaison to the Homeland Security Advisory Council; and Mr. Carlos Kizzee, counsel to the Homeland Security Advisory Council for their efforts in accommodating the very tight and challenging schedule demanded by this task.

MEMBERSHIP

Steven Abbot, ADMIRAL, UNITED STATES NAVY (RET.), PRESIDENT AND CEO
Navy – Marine Corps Relief Society

Dr. James Carafano, SENIOR RESEARCH FELLOW
DEFENSE AND HOMELAND SECURITY, THE HERITAGE FOUNDATION

Dr. Dan Gouré, VICE PRESIDENT
THE LEXINGTON INSTITUTE

Glenda E. Hood, SECRETARY OF STATE
THE STATE OF FLORIDA

Bruce Lawlor, MAJOR GENERAL, UNITED STATES ARMY (RET.), CHAIRMAN AND CEO
COMMUNITY RESEARCH ASSOCIATES, INC.

Rob Quartel, CHAIRMAN AND CEO
FREIGHT DESK TECHNOLOGIES

Seth Stodder, ATTORNEY AT LAW
AKIN, GUMP, STRAUSS, HAUER & FELD, LLP

Bruce Stubbs, DIRECTOR, SECURITY STRATEGIES AND POLICIES
CENTER FOR SECURITY SRATEGIES AND OPERATIONS, ANTEON CORPORATION

Jack Williams, PRESIDENT & COO
ROYAL CARIBBEAN INTERNATIONAL AND CELEBRITY CRUISES

EXECUTIVE SUMMARY

On December 21, 2004, President Bush signed National Security Presidential Directive-41, (NSPD-41) also entitled Homeland Security Presidential Directive-13 (HSPD-13). NSPD-41 / HSPD-13 calls for a comprehensive national security maritime strategy consolidating U.S. Governmental maritime security and strategy policies into a seamless comprehensive national effort. The Maritime Security Policy Coordinating Committee is the intergovernmental committee implementing the policies associated with NSPD-41 / HSPD-13. The National Maritime Security Working Group within that committee requested that the Homeland Security Advisory Council (HSAC) support the implementation effort by providing the sole consensus input on specific plans under development for implementation of NSPD-41 / HSPD-13.

In response to that request, the HSAC created the Task Force on the Implementation of a Comprehensive National Strategy for Maritime Security (hereafter "Task Force on HSPD-13" or "Task Force"). The HSAC charged the Task Force on HSPD-13 to review the plans submitted for consensus input, and to remain constituted to support the development and implementation of the national security maritime strategy. The Task Force empanelled and awaited presentation of the implementation plans for which consensus input was desired.

The Task Force's deliverable of consensus input was predicated upon receipt of those specific implementation plans. Due to understandable delays associated with the National Maritime Security Working Group's efforts in developing their draft implementation plans, the Task Force received the Maritime Transportation Security Implementation Plan, the Maritime Commerce Security Implementation Plan, and the Maritime Infrastructure Recovery Implementation Plan shortly before their meeting. Additionally, law and regulatory policy governing Federal advisory committees required input on this document be presented for deliberation to the HSAC and the results of that deliberation to the Secretary of the Department of Homeland Security. In order to meet the time frame required by the National Maritime Security Working Group, the amount of time available to the Task Force for detailed review, analysis, and presentation of their recommendations was severely limited.

This Task Force report does not incorporate or expressly reference any materials provided it for review. The Task Force recognizes that the United States Government provided it with pre-decisional documents for advisory comment. Accordingly, the Task Force has chosen to refrain from incorporating into this report or specifically referencing within their comments any portion of the content provided for their review.

In this report, the Task Force provides meaningful observations and input intended to prove beneficial to those responsible for drafting the final implementation plans submitted for our review. While some of the observations may seem purely critical in form, the Task Force believes that it is important to recognize that the successful drafting and implementation of National Security Maritime Strategy plans will ultimately be judged by how they are embraced and eventually implemented among the federal, state, local, tribal, and private sector stakeholders involved in the maritime community.

The plans reviewed by the Task Force are a very general and broad set of recommendations. The final challenge of the Maritime Security Policy Coordinating Committee is turning them into actionable plans capable of implementation by the Private Sector in harmony with all the relevant agencies at the federal, state, local, and tribal levels.

The Task Force notes that the security and resilience of the maritime industry is an extremely important component within our nation's efforts to securing our homeland from the consequences of all hazards including terrorists attacks and natural disasters. As such, the Task Force wishes to commend the excellent collaboration and foresight demonstrated in the development of these plans to date. The Task Force also seeks to encourage those involved with this most important effort to persist towards finalization of a plan that can be a model of how the public and private sectors must continue to work together to develop and successfully implement sustainable programs designed to promote the resilience of governmental systems, key resources, businesses, and industries that together constitute critical infrastructure vital to our economy and the freedoms that we enjoy within the United States of America.

FRANK J. CILLUFFO

Homeland Security Advisory Council Staff

Dan Ostergaard, ***Executive Director***

Katie Knapp, *Special Assistant to the Homeland Security Advisory Council*

Rich Davis, *Director, Academe and Policy Research Senior Advisory Committee*

Jeff Gaynor, *Director, Emergency Response Senior Advisory Committee*

Mike Miron, *Director, State and Local Officials Senior Advisory Committee*

Candace Stoltz, *Director, Private Sector Senior Advisory Committee*

Carlos Kizzee, *General Counsel Liaison*

Comments on the Maritime Transportation Security Implementation Plan

The Maritime Transportation Security Plan seeks to enhance U.S. national and homeland security interests in balance with the interests of national and international trade and the free flow of commerce. The integration and alignment of all U.S. maritime security initiatives into a cohesive national effort that involves stakeholders at the federal, state, local, tribal, and private sector level is an inherent component of this critical objective.

The Maritime Transportation Security Plan was the most mature of the three plans presented to the Task Force. Noting that all three plans had a diverse structure and format, the Task Force recommended that every plan be structured in a common format so that the goals and tasks in the Plan could easily be cross-referenced from one to another. The Task Force recommends the Maritime Transportation Security Plan as the most adequate model for the others to follow. While the Task Force found the tasks outlined in the Maritime Transportation Security Plan (the "Plan") to be adequate, the Task Force did note that the Plan lacked sufficient specificity. The following are specific concerns noted by the Task Force:

1. ***Responsibilities not Assigned***. Responsible organizations for implementing certain recommendations were not identified. For example, it is not clear who will be responsible for establishing and maintaining the Maritime Domain Security Risk Information System. Nor is it clear whether this System is a "green field" effort, or to be built on the efforts of other government agencies already in the business (the U. S. Coast Guard, the Department of Defense, Customs and Border Protection, etc). In addition, the "recommendations" should be called "requirements;" tasks that must be performed by the federal government as opposed to optional activities.

2. ***Lack of Performance Metrics***. No clear metrics are identified in the Plan for judging successful implementation. As an example, one particular recommendation required the State Department to assume a leadership role in coordinating with international stakeholders, but no measure was identified to assess the success of that effort.

3. ***Credentialing of Recreational Boaters Questioned***. Credentialing initiatives such as building on the Transportation Worker Identification Credential are worthwhile. The Task Force noted that some aspects of the recommendations related to credentialing required further study. While it might be useful to credential boaters trafficking in selected "high security areas," it is not clear that credentialing all recreational boaters would be useful or worth the cost. On the other hand, credentialing of persons involved in non-asset licensed maritime commerce activities (e.g. freight-forwarders) should be considered.

4. ***Maritime Exercise Requirement Needs More Fidelity***. The scope, objectives, and responsibility of the maritime exercise requirement should be better defined and keyed to evaluating the essential capabilities identified by the Plan (e.g. measuring the capacity to achieve maritime domain awareness). In addition, the exercise program for the Maritime Transportation Security Plan should be harmonized with the training requirements of the other plans. Consider one exercise plan to support the family of plans.

5. ***Stakeholder Coordination Recommendation Insufficient***. Removing barriers to effective information-sharing is essential to stakeholder coordination. The Task Force noted that one recommendation focused on the "process" of communicating rather than on specific means to overcome barriers to effective stakeholder coordination. There should also be specific requirements in that particular recommendation to ensure that information-sharing initiatives and policies are consistent with homeland security information-sharing efforts in areas such as the Freedom of Information Act, Protected Critical Infrastructure Information, and classified intelligence.

6. ***Recommendation for Training Ports in Developing World is Inadequate***. One recommendation in this Plan calls for increasing training assistance to ports in the developing world. Training is inadequate without assistance that addresses basic governance, human capital, economic, and infrastructure issues. The Plan should require integration of assessment, training, and foreign assistance programs into a coherent, strategic plan to engage selected states in enhancing their capacity to participate in international maritime security regimes. The Plan should also consider engaging other key allies to develop similar programs and synchronize them with U.S. efforts.

7. ***Education not Addressed***. Professional development and education for federal, state, and local officials, as well as the private sector will be essential for implementation of recommendations. This requirement should be addressed by the Plan. In particular, the concept "risk management" is not well understood and should be taught as a core competency in any maritime security professional education program. Additionally, an initiative similar to the Defense Department's "Goldwater-Nichols[1]" is required to ensure assignments, education, and accreditation of professionals that understand all aspects of the public-private maritime domain.

8. ***Security Technology Development Initiative lacks Focus and Specificity***. The overwhelming lion's share of this effort should be focused on stand-off nuclear detection.

9. ***Plan Overly Focused on Seaward Threats***. Inadequate attention given to threats to ports from the landward side. More emphasis on integration of law enforcement, domestic counterterrorism, and local intelligence and information-sharing is needed.

10. ***Prioritization Not Clear***. The Task Force noted that one particular figure implicitly suggested how efforts should be prioritized, but the actual prioritization was not clearly articulated in the recommendations.

11. ***Inventory of Ownership May be Needed***. Consider requiring an inventory of who has ownership responsibility for assets, infrastructure, and activities, at the federal, state, local, and private sector level, means to model their interaction, and whether such a tool and inventory list would be useful in managing and coordinating security activities in the domain.

[1] A reference by the Task Force to the Department of Defense's implementation of the Goldwater-Nichols Department of Defense Reorganization Act of 1986.

12. ***Funding Observation Needs to be Restated***. The Task Force noted a funding observation within the document that was not useful. A strong statement needs to be included for the federal government to maintain consistent levels of funding with consistent risk-based priorities for port security grants, to establish a predictable business environment that will allow public and private sector leaders to determine how to best invest for the future. On the other hand, the funding implications of the other recommendations in the Plan require greater fidelity. New funding requirements must be identified and the Office of Management and Budget tasked to assess their suitability, feasibility, and acceptability. The Plan should identify alternative recommendations of critical new funding needs that will not be met, and should determine a means to prioritize unfunded requirements. There was also a view that, while certain mandates might well require federal funding, other mandates or standards could well fall within the area of commercial responsibility alone depending upon whether they were good practices, risk related, etc.

Comments on the Maritime Commerce Security Implementation Plan

The Maritime Commerce Security Plan seeks to improve the security of the maritime supply chain in order to lower the risk that components of that chain might be used to support terrorism and other criminal, unlawful, or hostile actions. By promoting international maritime supply chain security, the Maritime Commerce Security Plan seeks to reduce the vulnerability of the maritime domain and protect lawful maritime commerce while maintaining close integration among all other plans and initiatives related to the National Strategy for Maritime Security.

The Maritime Commerce Plan generally reads well, although some of its assumptions about the facts of the maritime infrastructure are arguable. Much of it is taken up with a recitation of programs already underway, many that come across as stand-alone programs without any overarching strategic framework. As a result, the Plan fails to present a clear argument and well-defined path towards more effectively addressing perceived security vulnerabilities in the maritime commerce system. Given the dynamic and presumed long-term danger of the threat, there is too much intellectual complacency contained in the Plan. That being said, the Task Force supports most if not all of the specific recommendations of the strategy with the caveat that we believe DHS specifically or the U.S. Government generally should be cited as the overarching locus of these activities rather than Customs and Border Protection. We believe this to be necessary given the important roles of other DHS agencies (such as the Coast Guard), as well as other Cabinet Departments (such as the Department of Energy and Department of Defense). The Task Force also believes that there needs to be a much greater department-level commitment reflected in this strategy.

1. ***Need for higher level/holistic view of the strategy that is connected to other strands of the national homeland security strategy***. While the Maritime Commerce Security Plan begins by stating that the Plan is not about trade compliance, many of the programs recited and the strategies underlying them are predicated on a compliance perspective. While there are tactical similarities, much of the threat risk is opportunistic and contextual and may not be particularly vulnerable to traditional validation techniques.

2. ***Too U.S. and Border-focused***. While it is true that a focus of maritime security is port and border-centric, e.g. centered mostly on the security of commerce directly entering the United States, any attack anywhere on the global system will have an impact on both the US and the global economy. The Plan needs to more actively place the security of maritime commerce in the broader context of securing global commerce and globalization generally. Given the economically dynamic, intermodal, and networked nature of global commerce, maritime commerce security cannot be viewed in a vacuum, or simply as a function of the narrower (but obviously important) goal of preventing terrorist weapons from entering the United States.

3. ***Too Maritime-focused***. While it is true that this is a maritime security Plan, no maritime cargo begins, ends or moves exclusively by water or in the maritime domain. All water-borne cargos begin and end with trucks, trains, domestic water, etc and inside a country with a person, somewhere. The focus on US-bound water cargo also blinds it to other possibilities for terrorist delivery of weapons of mass destruction via water – such as via a cargo container to a Mexican port, which is then unloaded and its contents driven across the land border. The Plan needs to integrate into domestic and international surface security systems.

4. ***Threat of Nuclear Terrorism Needs to be Clearly Identified as Preeminent***. While the Plan provides a good discussion of the general context in which the threat occurs, (exponential growth in world trade) and correctly identifies the security of maritime commerce as an issue of both "port" and general national security, it fails to make a convincing case for container-borne maritime commerce as a likely means of bringing a weapon of mass effect or components into the country. It is also not analytical about the tactics driving this assumption or the cost of a successful terrorist incident/attack. It may very well be that the threat of the "nuke in a box" seems to be the preeminent threat the maritime commerce strategy should be addressing, but there is little argument or intelligence basis underpinning this assumption. The threat of nuclear terrorism should be clearly identified as preeminent if it in fact is.

5. ***Need for a Net Assessment of the Cost/benefit of Nuclear Detection Programs***. The cost and reality of the threat need to be measured against the cost of the supposed deterrence. In terms of solutions, the Plan is conflicted on this issue. While it cites the need to "push the borders out" and to identify threats well before they arrive at U.S. shores, its solution is to deploy Radiation Portal Monitors (RPMs) domestically, at U.S. seaports. The shortcomings of this DOA ("detection on arrival") strategy are recognized in the Plan; but its proposed solution, the Department of Energy's Megaports Initiative (which aims to deploy RPMs in foreign seaports) is likewise limited in scope and science. A better approach might be to simply state the policy objective for dealing with the priority mission of preventing nuclear terrorism (as identified within the Plan); namely that 100% of all sea containers should be effectively screened for radiation before arrival at U.S. seaports. There may be other ways of addressing the threat or of adding layers of defense (*e.g.*, passive or active detection technologies that are deployed at-sea, on the ships, or on or within the containers themselves).

6. ***Over-emphasizes Container Security to the Detriment of an Overall Maritime Solution***. By focusing on *containerized* commerce alone, the United States Government implicitly suggests alternate methods of a weapons of mass effect breech, which might include, for example, bulk or break-bulk shipments, project cargos, pleasure craft, small ships, domestic barge diversions, etc. The Plan needs to explicitly identify the potential for the non-containerized threat and provide a process (including satisfying measures in the short term) for dealing with those threats should they, in the minds of experts, exist.

7. ***Misplaced Focus on In-transit Security***. While in-transit security is clearly an element of a global logistics strategy, it is only a piece of the puzzle, in a complex multi-party, multi-transaction environment. The strategy needs to reach across the process from order to manufacturing, finance, transportation and distribution processes and players. It would be unfortunate to secure the trip of a nuclear device already packaged so well that it successfully arrives within the United States.

8. ***Need for a Net Assessment of the Customs-Trade Partnership Against Terrorism, Including the Development of Real Success Measures***. The Customs-Trade Partnership Against Terrorism (C-TPAT) is predicated on a notion of supply-chain best practices, known parties, and self-assessment with limited government validation. Government success is declared largely in terms of "membership," not actual validations or security. There is no reference to C-TPAT's vulnerabilities, including the lack of clear commercial incentives for its adoption. Another vulnerability is identified by prevailing questions regarding the precision of the validations in light of the threat of a "clean" terrorist embedding him or herself in a "known shipper" to C-TPAT importers; a potential concern given the multi-year timeframe of terrorist planning evidenced by the attacks on September 11, 2001. There needs to be a net assessment of C-TPAT, including the development of real success measures that extends beyond merely counting the number of parties that have signed up for C-TPAT (the apparent current standard). While the Task Force generally endorses C-TPAT as an initial effort, there needs to be more thinking about the program's vulnerabilities, utility, measures, and penetration strategies. If we presume that the threat is real and the program is a viable deterrent, there should be an explicit strategy to incorporate C-TPAT or successor programs into a broader, more embedded system of frequent accountability and audits.

9. ***Need to Develop an Approach Leveraging Licensed Third Party and Private Inspection Capabilities with the Government in the "Inspect the Inspector."*** The Plan reflects no new thinking here, or alternative approaches – including the potential use of third parties to speed up, make more rigorous, or increase the number of verifications. Customs and Border Protection cannot be everywhere all of the time. Moreover, the focus of the Plan, the DHS, and the Department of Energy on large "mega" ports comes at the detriment of third world and developing countries, many whose growth democratically and economically we support (in part as a solution to terrorism), yet which themselves are considered suspect countries of origin. To the extent that we are seeking to detect smuggled nuclear weapons or materials before they arrive at a U.S. seaport, it makes little sense to limit the deployment of detection equipment to large ports that ship commerce to the United States…our enemies can simply ship a mass-effect weapon from a smaller

port that is not equipped with radiation detection equipment. Also, to the extent that an element of the Plan is increasing targeted physical inspections, it needs to develop an approach that may leverage licensed third party and private inspection capabilities as a “force multiplier,” with government activities focused on "inspecting the inspectors."

10. ***Mandating Technologies Without a Clear Business Case or a Clearly Defined and Mandated National Security Requirement***. It is not surprising, given the Plan’s emphasis on in-transit container security, that the Plan cites a need to develop “smart containers,” the ostensible purpose of which is to detect tampering and intrusions. Radio Frequency Identification (RFID) technology to track shipments, and electronic as well as stronger physical locks on containers are likewise explicit parts of the strategy built around container (rather than shipment) security. These aspects of the Plan appear to lack a clear and articulated basis in either the threat or in its mitigation. Nor is it evident that there exists an independent commercial benefit (e.g., business strategy) for most parties in trade to implement these “technologies.” While logic suggests that for certain high value cargos better in-transit security and tracking of containers may be a good idea (and may be good business practice for inventory control), “smart containers” and many other seal and tracking technologies may be solutions in search of a problem. There should be no recommendation or mandate for so-called “Smart Containers,” RFID and other tracking and high-tech physical solutions without a clear business case or in the alternative a clearly defined and mandated national security requirement focused on the conceivable threat that our nation’s enemies may intercept a container mid-stream to insert a weapon (as opposed to deploying the weapon in the container at its point of origin).

11. ***Need for a Clear Outline of Private Sector Responsibilities for Cargo Security***. While the Plan states a belief in the threat and possibility of a terrorist act using the maritime commerce system, it neither presents nor defines anything of adverse consequence inside that system, undermining not only the credibility of the threat itself but of the suggested program counter-measures. In our experience, too many parties at the company level within the commercial sector find the supposed threat underwhelming. Assuming the threat is real and the risk is high enough, the Plan should clearly outline the Private Sector responsibilities for cargo security in order to begin ingraining necessary security measures into business practices.

12. ***Need for Clear Definitions of Terms-of-art***. The Plan emphasizes the reality that not all shipments can be physically “inspected,” consistent with permitting the smooth flow of global trade – nor should they under a rational risk strategy, given that most present no threat. Rather, intelligently securing global commerce means managing risk, and using advance information and intelligence to target the highest risk shipments for greater scrutiny. We need a clear definition of terms such as "inspection."

13. ***Potentially Overstates the Effectiveness of Current DHS Targeting Programs***. The Task Force strongly supports the recommendations in the Plan for better and additional data collection throughout the global supply chain. The Task Force also supports cooperation with other United States Government agencies (including not only the U. S.

Coast Guard, but the Department of Defense, the Department of Energy, the Department of Commerce, etc). However, we strongly suggest that DHS refine the distinctions between compliance and threat analytics. The current targeting approach continues to rely primarily on advance *manifest* information, the experience of Customs and Border Protection officers, and the intelligence reflected by the databases, targeting programs, and rules managed by the National Targeting Center. Manifest data is known to be inadequate and unreliable. Customs and Border Protection officers (among most if not all of law enforcement) are inexperienced with even known terrorist smuggling patterns. Those factors and the recent experiences with catastrophic national intelligence failures (9/11 and Iraq weapons of mass destruction) suggest that targeting processes need further review or some other security layers that are not dependent upon targeting. As an example, mechanisms for running 100% of all shipments through nuclear radiation detection screening before they arrive in the U.S. need to be expeditiously put into place as an additional fail-safe layer (assuming that they pass the risk and probability test). The probability of detection via risk analytics also needs to be explicitly linked to the scope and depth of other layered programs, including physical, process, and people-based programs. We support continued research and testing of new capture and risk assessment technologies, particularly those aimed at developing commercial intelligence capabilities across the supply chain.

Comments on the Maritime Infrastructure Recovery Implementation Plan

The Maritime Infrastructure Recovery Plan seeks to establish a coordinated approach in areas within or adjacent to seas, oceans, and navigable waterways for the rapid recovery of maritime transportation capabilities from incidents of national significance bearing the potential to adversely affect the U.S. economy.

The Maritime Infrastructure Recovery Plan (MIRP) provided some unique and beneficial insights to how industry should respond to any disaster which could cause an interruption to the free flow of commerce whether it be cargo or passenger related. The Plan, however, was viewed in general by the Task Force as being too vague and probably the weakest of the three plans presented to the Task Force. It was clear that there were a number of major issues regarding clarity of objectives and its relevance to how this Plan integrates with the other two plans, as well as other governmental agencies (i.e. the Federal Emergency Management Agency) and plans. Specific comments regarding the Plan were as follows in no specific priority:

1. ***Private Sector Involvement***: Perhaps the most salient concern revolved around the fact that the role of the private sector in the Plan was yet to be determined. The Task Force noted that this was unacceptable since the vast majority of the critical infrastructure is owned and operated by the private sector. It was noted that a number of members of the private sector had been consulted prior to the drafting of the document, but evidence of the Private Sector’s input was not obvious in this draft. Having said that, regardless of the level of involvement of the Private Sector in the preparation of the Plan, the Plan

itself notes that the role of the Private Sector in the MIRP is yet to be defined and the committee viewed this as a serious shortcoming that needed to be addressed in this draft.

2. ***Is this a Plan***? As presented, the Plan actually appeared to be a broad set of recommendations as opposed to a plan that would normally encompass a set of definitive objectives, targeted deadlines for accomplishment, and clear accountability for ownership of those objectives. The MIRP also lacked any metrics to determine success of the Plan. Until these concerns are addressed in the final draft, the Task Force questions the long-term sustainability of MIRP and its relevant value to the Maritime Industry.

3. ***Where's the Money***? Should MIRP be adopted as part of HSPD-13, there is currently no mechanism in place to fund the many initiatives proposed in the Plan. This was not unique to MIRP as it was clear that funding did not exist for the other two Plans. The Task Force expressed concern that enormous resource and focus was being spent to draft critical plans for the maritime industry which, in all likelihood, would lack the funding necessary to effectively execute the plans. While this concern may extend beyond the role of the Task Force, it was generally agreed that this issue needed to be raised to those responsible for the overall drafting and eventual successful implementation and execution of these plans.

4. ***Business Continuity and Disaster Recovery***: The MIRP outlined both specifically and indirectly a number of initiatives and recommendations which industry should/can take as it relates to their Business Continuity and Disaster Recovery Plans. The Task Force noted that the 9/11 Commission Report issued in 2004 recommended to the private sector that NFPA-1600 and ANSI be used by the private sector as the "standard" for developing Disaster/Emergency Management and Business Continuity Programs. The Task Force felt it would be prudent for the MIRP to, at a minimum, cross-reference the 9/11 Commission recommendations in the final draft. A more robust plan would include recommendations and programs that seek to increase the system resiliency within the maritime community beyond the minimum standards of business continuity established in NFPA-1600.

5. ***Functional Exercises***: The MIRP specifically recommends that "Functional Exercises" be conducted between a variety of federal agencies and the private maritime sector over the next several years. The Task Force recognized the importance of these exercises in the overall success of any infrastructure recovery program. However it was unclear what was meant by "Functional Exercises", and without careful planning with the private sector, the sheer number of these required exercises could prove to be overwhelming. Given the importance of these exercises and simulations between the public and private sectors, the Task Force recommends that the MIRP, in its final draft, clearly outline and define how these important exercises will be coordinated and executed with the private sector.

6. ***MIRP needs to be more Network Focused***: There was a general consensus that MIRP in its current state was too incident focused and not sufficiently focused on networks. Without focusing its objectives on strengthening the resiliency and recovery systems in

the maritime environment, the Plan is overly duplicative of the National Response Plan and may not be seen by the maritime community as adding value to maritime security.

7. ***Overlap and Redundancy:*** In reviewing the document, it became apparent to the Task Force that there was an enormous amount of overlap and redundancy with other government plans and agencies. This creates a concern that the document's relevancy will be at question given the number of other documents and plans that either directly or indirectly address many of the same objectives of the MIRP. This has been a long standing concern of the private sector. There is a common belief among industry that new, relevant, and useful information/content will accompany the introduction of a new governmental plan like MIRP. The Task Force strongly believes that this may not be the case with MIRP. Regardless, the document's relevancy should be demonstrated by clearly illustrating how MIRP is adding value beyond other existing documents which are addressing the same concerns. To provide one specific example, there was considerable discussion of how MIRP was providing any relevant value beyond what the Federal Emergency Management Agency already does in providing disaster recovery expertise and funding. In the absence of such clarity, the publication of MIRP will likely result in nothing more than creating additional confusion and frustration within the sector; a result that clearly needs to be avoided given this important effort.

8. ***System Recovery and Start-Up:*** While MIRP addresses the whole issue of system recovery it does not specifically address when or how a port, waterway, or any other critical maritime infrastructure would be restarted following a temporary shutdown and the applicable protocol to be used in that process. The Task Force recommends that more thought be given to this aspect of the recovery process, clearly outlining as best as possible how the private sector would coordinate their efforts with appropriate federal, state and local agencies to resume operational services once the safety of the public, critical infrastructure and other private assets have been considered secured.

9. ***Worth Noting:*** The Task Force noted that the recognition of the importance of reserve capacity (and capability), national salvage capability and the recovery resources and assets of other countries was an insightful piece of MIRP which provided significant value to the overall document. The Task Force recommends that these three points be further developed in the final draft.