Report of the
Defense Science Board Task Force
on
Critical Homeland Infrastructure Protection

January 2007

Office of the Under Secretary of Defense
For Acquisition, Technology, and Logistics
Washington, D.C. 20301-3140

This report is a product of the Defense Science Board (DSB). The DSB is a Federal Advisory Committee established to provide independent advice to the Secretary of Defense. Statements, opinions, conclusions, and recommendations in this report do not necessarily represent the official position of the Department of Defense.

This report is UNCLASSIFIED and releasable to the public.

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	January 2007	Final, January 2007

4. TITLE AND SUBTITLE
Critical Homeland Infrastructure Protection

5. FUNDING NUMBERS

6. AUTHOR(S)
Dr.'s Miriam John and Ronald Kerber
Task Force Co-Chairmen

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Defense Science Board
3140 Defense Pentagon, Room 3C553
Washington, DC 20301-3140

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Defense Science Board
3140 Defense Pentagon, Room 3C553
Washington, DC 20301-3140

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION AVAILABILITY STATEMENT
A: Open Distribution

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

14. SUBJECT TERMS

15. NUMBER OF PAGES
37

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclass	Unclass	Unclass	

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301-3140

DEFENSE SCIENCE
BOARD

Jan 10, 2007

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY & LOGISTICS

SUBJECT: Final Report of the Defense Science Board (DSB) Task Force on Critical Homeland Infrastructure Protection

I am pleased to forward the final report of the DSB Task Force on Critical Homeland Infrastructure Protection, chaired by Dr. Mim John and Dr. Ronald Kerber. The study examined best practices to protect and enhance the security of US homeland installations. The Task Force's observations and recommendations are consistent with previous DSB studies, and if implemented, will improve the Department's capabilities of protecting US homeland installations for the future.

Since the 2003 DSB Summer Study on Department of Defense (DoD) Roles and Missions in Homeland Security, DoD has made strong efforts in expanding its role in protecting installations from various modes of attack. However, through the course of the study, the Task Force realized that homeland defense protection covers a broader scope than the range of topics requested by the Terms of Reference. Larger issues related to protecting national security mission critical capabilities warrant consideration, and the Task Force recommends that the Secretary of Defense direct an additional study to focus on these concerns.

I endorse all of the Task Force's recommendations and encourage you to forward to the Secretary of Defense.

William Schneider, Jr.

Dr. William Schneider, Jr.
DSB Chairman


DSB

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301-3140

DEFENSE SCIENCE
BOARD

MEMORANDUM FOR THE CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Final Report of the Defense Science Board (DSB) Task Force on Critical Homeland Infrastructure Protection

Attached is the final report of the DSB Task Force on Critical Homeland Infrastructure Protection. The report emphasizes the challenges facing the Department of Defense (DoD) with respect to protecting US homeland installations. This Task Force determined that the Department has made progress in expanding its role in homeland security since the 2003 DSB Summer Study on DoD Roles and Missions in Homeland Security, but more areas need to be included in homeland defense protection. The following areas of infrastructure protection were examined:

- DoD/Department of Homeland Security (DHS) Coordination;
- DoD and Defense Industrial Base (DIB) Security;
- Risk Management and Resource Allocation;
- Understanding Infrastructure Interdependencies;
- Best Practices;
- Systems and Technologies;
- Standards and Metrics; and
- Information Sharing.

Major recommendations include improved coordination and integration between DoD and DHS in the areas of: planning, research and development (R&D), acquisition, operations, and training, as well as setting policy objectives to manage risks for critical assets. With respect to best practices, the Task Force recommends DHS(IP) to monitor, collect, and share best practices for all sectors, especially to owners of critical facilities. The Task Force also recommends to DoD that DDR&E be assigned to develop a joint R&D program with DHS Science and Technology (S&T) to address infrastructure security and protection technical challenges. Most important, DoD should develop an integrated program to address policies, practices, and procedures for mitigating risks to critical assets and operations, allowing exemptions to acquire and protect sensitive DIB information where necessary.

These findings and recommendations are outlined in the following report. Though the recommendations cover a large scope, larger issues related to protecting national security mission critical capabilities should strongly receive consideration, and the Task Force recommends that the Secretary of Defense direct an additional study to focus on these other concerns. The Task Force

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301-3140

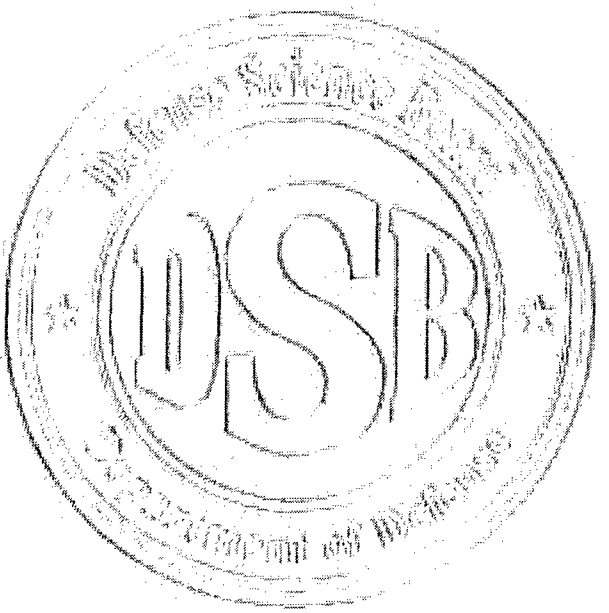
DEFENSE SCIENCE
BOARD

urges the senior leaders of the US government to implement the recommendations at the earliest opportunity.

Dr. Miriam John
Co-Chairman

Dr. Ronald Kerber
Co-Chairman

TABLE OF CONTENTS



I. EXECUTIVE SUMMARY

TASKING AND SPONSORSHIP

The Defense Science Board (DSB) was asked jointly by the Department of Defense (DoD) and the Department of Homeland Security (DHS) to establish the Critical Homeland Infrastructure Protection Task Force to assess best practices for protecting US homeland installations and recommend various approaches to enhancing security and protection of these facilities, to include:

- Reviewing existing best practices, to include risk management approaches, in force protection and security at civil, industrial, and military complexes;
- Assessment of shortfalls and deficiencies associated with operational security;
- Identification of promising technology and/or processes that will enhance security;
- Recommendations for methods for reducing overall manpower requirements without relinquishing robust security measures;
- Identification of issues and recommendations for the balance between military and private responsibilities for critical facility protection; and
- Understanding security standards and metrics and identification of any gaps. [1]

PRINCIPAL FINDINGS AND RECOMMENDATIONS

DoD has made notable progress since the DSB recommended that it expand its roles in homeland security and defense in the 2003 Summer Study on *DoD Roles and Missions in Homeland Security*. However, this area is still viewed by many as a new mission for the Department, and as such, much still remains to be done. The Task Force offers the following findings and recommendations, with respect to the focus on infrastructure protection.

A. DoD/DHS Coordination

Many levels within DoD support and pursue a strong partnership with DHS in areas related to infrastructure protection, but relationships tend to be *ad hoc*, without comprehensive engagement and with fragmented accountability. This results in gaps, overlaps, and poor integration. The Task Force commends the recent action by OASD (HD)/DCIP[2], in which a liaison to the Infrastructure Protection Office at DHS has been identified to help remedy the situation, but much more is needed.

The Task Force recommends that:

[1] See Appendix A for a complete statement of the Terms of Reference.

[2] Office of the Secretary of Defense for Homeland Defense/Defense Critical Infrastructure Protection.

- The Deputy Secretaries of DoD and DHS direct that coordination and integration between the two departments be institutionalized through a formal Memorandum of Understanding (MOU) with a scope that includes planning, research and development, acquisition, operations, and training;
- The ASD (HD) in DoD and A/S IP in DHS be assigned to implement the MOU, and the Deputy Secretaries of DoD and DHS annually review progress.

B. DoD and Defense Industrial Base (DIB) Security

For DoD owned facilities, dependence on non-DoD infrastructure is not entirely known. In fact, until recently, the Department lacked policies and standards to guide installation commanders in securing, or creating contingencies for, infrastructure on which they depend.[3]

The Task Force recommends several actions:

- OASD (HD)/DCIP should oversee the characterization of the defense sector infrastructure dependencies, promulgate risk mitigation guidance, and establish uniform Defense Critical Infrastructure Protection (DCIP) standards;
- The Services should develop and implement plans to mitigate risk to an acceptable level and should provide an annual update of progress to the Deputy Secretary through the ASD (HD);
- Installation commanders should develop local assessments of infrastructure dependencies and implement risk mitigation plans consistent with guidance and standards; and
- The Commander of NORTHCOM should integrate installation dependencies and infrastructure risk mitigation as a matter of command emphasis in his interaction with the Services in accordance with established OSD guidance and policy. Other Combatant Commanders should provide similar emphasis for DoD installations in their areas of responsibility.

With respect to the Defense Industrial Base (DIB), DoD is often not the primary customer, and the owner's business objectives may be at odds with DoD security objectives. The problem is exacerbated by the many and growing critical assets overseas.

The Task Force recommends that:

- OASD (HD)/DCIP set policy objectives for managing the risks of critical DIB assets;
- USD (AT&L)/Industrial Policy review and revise, if necessary, Defense Federal Acquisition Regulations (DFAR) to ensure compliance with Policy objectives;

[3] DoD Directive 3020.40, "Defense Critical Infrastructure Program," signed August 2005, assigns CIP responsibilities at all levels across the department

- Agencies, offices, and Service organizations in DoD with DIB critical links should review existing contracts of the critical DIB assets to ensure policy objectives can be addressed.

C. Risk-Based Approach to Decision Making for Resource Allocation

Sound risk management and mitigation considers threat (capability and intent), vulnerabilities, consequences, and mitigation options. The Task Force discovered that the Department is far from practicing a risk-based approach. The Department conducts in excess of two dozen different vulnerability-focused assessments, but falls short in addressing full risk assessment that would include threat, consequences, and mitigation options. Moreover, DoD further complicates the situation by implementing programs in response to specific threats, events or concerns (e.g., AT/FP, HD/CIP, COOP, Guardian for CBRNE, cyber, etc.), each of which generates its own assessments, focuses on compliance rather than performance, and deals with current threats. In this context, it should not be surprising that current resource allocations within DoD are not matched to risk. DHS is shifting to a risk- based approach, but lacks consistent application of tools and methodologies.

The Task Force recommends that DEPSECDEF designate a lead for an integrated risk management and mitigation program with responsibilities to:

- Consolidate the many vulnerability assessment programs into one risk assessment program that includes performance based criteria, and considers the spectrum of current and future threats;
- Seek congruence of methodologies and tools with DHS (IP) and avoid duplication of effort;
- Help identify prudent risk mitigation measures and assess progress in achieving improved levels of security;
- Ensure deployment in a nested fashion from "global" to local;
- Evaluate resource allocation by infrastructure owners (both within DoD and the DIB) for consistency with risk assessments; and
- Assure timely cycling back through the process as conditions change.

ASD (HD)'s proposal for achieving mission assurance[4] should be considered for addressing these issues.

D. Understanding Infrastructure Interdependencies

DHS (S&T) is making important, but limited, investments to characterize and catalog the interdependencies among infrastructure sectors. The effort is further hampered by the lack of effective information sharing and protection mechanisms between the government and infrastructure owners.

[4] "Strategy for Homeland Defense and Civil Support," signed June 2005.

The Task Force recommends that:

- DHS (S&T and IP) accelerate characterization of infrastructure interdependencies and fold the results into analytical tools that can be used by sector owners, so that they can assess and implement mitigation measures to avoid sector failures due to the failures of a different sector;
- DHS (IP) implement protected information sharing methods that could accelerate mitigation planning at the local level; and
- DoD through OASD (HD)/DCIP seek priority for both of the above with DHS through an MOU with DHS; the MOU should address areas for collaboration to enhance understanding of infrastructure dependencies and establish a coordination mechanism for the development of tools to assess interdependencies and model cascading failures .

E. Best Practices

The identification of "best" practices proved impossible given the size and complexity of the nation's infrastructure. However, a number of exemplary practices and approaches were identified through offsite visits and targeted briefings. Examples include:

- New York City: Interoperability and integration
- Norfolk Naval Station and City of Norfolk: Military-civilian collaboration
- American Chemical Council: Industry standards
- Bonneville Power: Risk assessment and mitigation
- Financial sector: Intra-sector information sharing
- Telecommunications sector: Public/private cooperation
- Northrop Grumman: Application of information technology

The Task Force found that, at best, sharing of approaches and practices occurred through *ad hoc* mechanisms and/or word of mouth.

The Task Force observes and recommends the following:

- DHS (IP) should monitor, collect, and share best practices for all sectors, but especially for owners of critical facilities or nodes. The Government Coordinating Councils (GCCs) and Sector Coordinating Councils (SCCs) will play a pivotal role in all aspects of best practices by facilitating information sharing, assessing good and best practices, and establishing standards and guidance to be promulgated throughout the private sector and government agencies.;
- DoD can both benefit and contribute to this effort. However, DoD does not have a structure for coordinating the implementation of best practices. In the interest of protecting U.S. military readiness and capabilities, DoD should establish through OASD (HD)/DCIP a process that incorporates the identification, communication, and implementation of best practices as part of the previously recommended risk management and mitigation program.

F. Systems and Technologies

The Task Force had a difficult time finding examples of technology used to offset manpower commitments. Most examples are well-known – video surveillance, magnetic badge readers, limited biometrics, etc. Little investment[5] – and thus, little creative thinking – about potential technical solutions to improving security has occurred, yet the "Grand Challenges" are numerous, e.g.;

- Detection of terrorist surveillance activities;
- Standoff detection of CBRNE;
- Monitoring of "people of interest" while protecting civil liberties;
- Detection of hostile intent;
- Detection and denial of airborne threats; and
- Detection and denial of waterborne threats.

The Task Force recommends that the ASD (HD) and USD (AT&L) designate DDR&E to develop a joint R&D program with DHS S&T. Such a program should address and fund the "Grand Challenges," whose solutions will require top teams from academia, laboratories, government, and industry. In addition, this interagency program should support the adaptation of useful technologies from other military areas to Homeland Security. DoD and DHS must also support deployment of security systems and technology. This requires:

1. Integration of modeling and simulation tools;
2. Use of pilots to experiment with and refine new systems and technologies;
3. Development of CONOPS for Homeland Security applications; and
4. Training of operators in the field prior to systems deployment.

As the "technically tolerant" first user, DoD should be willing to provide sites for piloting new systems and technologies.

G. Standards and Metrics

DoD lacks objectives and standards for mitigating risks to critical assets. DHS (S&T) has established a Standards Program to develop and coordinate adoption of national standards and evaluation methods for equipment claiming to meet HS mission needs. The National Institute of Standards and Technology (NIST) has been enlisted to support the effort, and DoD has had limited engagement through OASD (HD)/DCIP. A comprehensive program, which addresses policies, practices, and procedures, as well as equipment and system performance, is needed.

[5] Neither DARPA nor DHS is investing for more robust or advanced solutions; limited near term maturation funds can be found in the interagency TSWG, DHS RTAP, DoD PSEAG and DOE security programs.

The Task Force recommends that:

- OASD (HD)/DCIP articulate clear DCIP objectives and develop standards and benchmarks for identifying and assessing DoD dependencies on critical infrastructure;
- OASD (HD)/DCIP work with ASD (SO/LIC) and USD (I) (through the Defense Security Agency) to promulgate standards for mitigating risks of critical assets both at home and abroad;
- OASD (HD)/CIP engage the DHS Standards Program regarding CIP analysis tools, components, systems; and
- OASD (HD)/DCIP, in consolidating risk assessment tools, should coordinate with the DHS effort with ASME RAMCAP to ensure a standardized approach for such assessments.

H. Information Sharing

DHS lacks sufficient mechanisms for protecting and sharing private sector information related to CIP operations and vulnerabilities, including lack of classification guidance and confused practices about handling "sensitive, but unclassified" information. DoD may require special exemptions to acquire and protect DIB proprietary or sensitive information. At the same time, DIB owners may be reluctant to share fully so long as impact and liabilities on them remains unclear.

The Task Force recommends that:

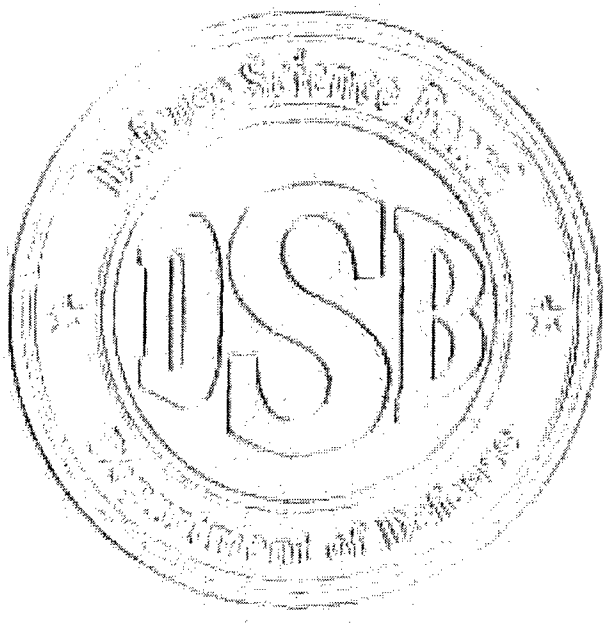
- DHS (IP) develop guidance and trusted mechanisms for information protection and inter-/intra-sector sharing; and
- OASD (HD)/DCIP work with the private sector to establish clear guidance and expectations for DIB critical asset owners.

I. Conclusion

The Task Force would like to add that as this study was performed on protecting critical infrastructure as outlined in the Terms of Reference (TOR) and viewed in the Department, it became obvious that a much bigger issue lies outside the protection of DoD critical facilities alone. A starting focus should be in the area of protection of the country and its military national security mission capability. This study was staffed and focused on the classical protection of critical facilities. Military strategy, policy, doctrine and planning can have much more significant impact on protecting critical mission capability by looking at the distribution of assets – i.e., limiting concentration of critical assets can protect mission capability much more than facility protection alone. This study has recommended reasonable beliefs in protecting critical military facilities, including the defense industrial base. A second view would consider policies and strategies for making facilities less critical rather than just protecting critical facilities. The Task Force recommends that the Secretary of Defense direct the staffing of such a study with the capability to look at the issue in this new light.

The straightforward statement of tasking to the Task Force belies the breadth and depth of effort required to address each task completely. Information gathering, while extensive, could not be comprehensive.[6] Nonetheless, a number of important themes and recommendations emerged that the Task Force believes will be useful to DoD and DHS leadership. These were summarized in the Executive Summary and will be described in more detail in the following sections.

[6] The reader will also note that the publication of the report lagged the initial phase of information gathering by the committee. The committee co-chairs were careful to assure that key points in the report were updated where necessary in order to assure currency of the findings and recommendations up to the time the report went into peer and security review.


DSB

II. INTRODUCTION

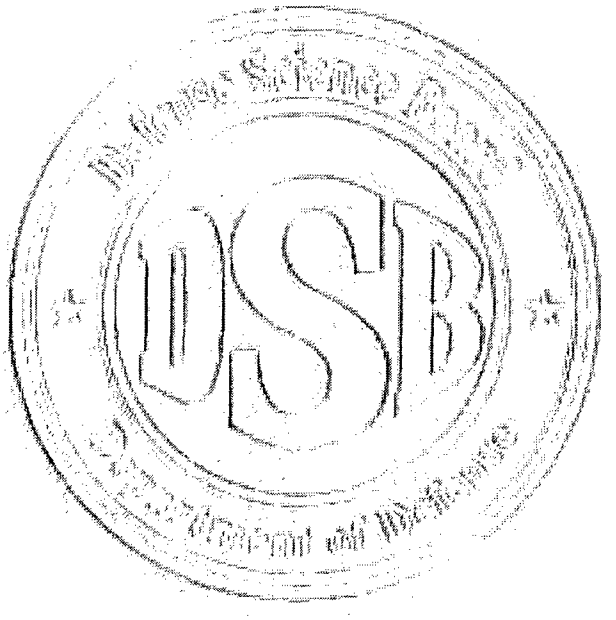
In the post 9-11 environment the nation has become much more aware of the potential vulnerabilities, and hence, security needs of many of its critical facilities and infrastructure. A number of important and generally useful efforts have been undertaken by the Department of Homeland Security (DHS) to help guide the owners of key assets in improving their security posture, and by the Department of Defense (DoD) for those assets for which it is directly responsible. As initial measures are settling in, leadership at both DHS and DoD is recognizing that assessments are needed to better understand our progress to date and to assure that further investments will be wisely made.

Within this larger context, several, more specific observations motivated the efforts of this Task Force. One is that the predominant reliance on "guns, guards, and gates" for protection of facilities and valuable assets, although expedient, is an expensive approach. Another is that most actions have been taken by individual facility and infrastructure owners in a relative vacuum from others in the same or similar situations. Best practices are not widely known and "good enough" not well understood. Yet another is the typically limited understanding by facility and infrastructure owners of the assets and infrastructure which they do not own, but on which they are dependent. The security of such assets and infrastructure may be as important as the security of their own.

Complicating organizational dimensions of critical facility and infrastructure protection at the national level is the relative lack of maturity of DHS programs and processes, and instability of the leadership and reorganization of the Infrastructure Protection Program. In addition, DoD itself is experiencing its own "growing pains" with the emergence of Homeland Defense as a major mission. New lead organizations, ASD (HD) and NORTHCOM, have been stood up in the midst of well established policy organizations and Combatant Commands, while a host of separate Service and Joint Staff groups have been created, largely independently, to address a wide array of operational issues.

The straightforward statement of tasking to the Task Force belies the breadth and depth of effort required to address each task completely. Information gathering, while extensive, could not be comprehensive.[7] Nonetheless, a number of important themes and recommendations emerged that we believe will be useful to DoD and DHS leadership. These were summarized in the Executive Summary and will be described in more detail in the following sections.

[7] See Appendix C for a listing of all briefings, tours, and discussions.


DSB

III. FINDINGS AND RECOMMENDATIONS

A. DoD/DHS COORDINATION

The DoD and DHS are working individually and together in a number of important ways to enhance the nation's homeland and national security. There are several high-level national strategy and policy documents that define the general roles and responsibilities of both agencies.[8] The general sense of the Task Force is that: (1) in contrast to several earlier DSB studies, many in DoD have come to recognize the strong role it needs to play in homeland security; and (2) leaders at the highest levels of the two federal agencies are supporting their partnership. The Task Force believes that this is also true at many lower levels within both agencies, but there is significant room for improvement. In the area of infrastructure protection where this Task Force focused, continuing to clarify roles and responsibilities, along with strong coordination of planning, research, training, operations, and acquisition, will enable both agencies to perform more effectively and efficiently. Such actions will help ensure complementary investments, plugging significant gaps that adversaries could exploit, and in the event of a terrorist incident, nearly seamless response and rapid recovery.

The Task Force's primary concerns were in the operational and programmatic areas. Working relationships exist, but are not uniformly institutionalized or formalized to a degree that ensures ongoing coordination and integration. Examples where integrated programs and operations are important for infrastructure protection include:

- DoD's Northern Command (NORTHCOM) and the DHS Transportation Security Agency (TSA), as well as the Federal Aviation Administration (FAA) and the airline and aviation industries, to protect the nation's airspace from attack, including the use of the nation's commercial and general aviation assets against us;
- The Navy and Coast Guard, along with the owners and operators of the nation's ports and shorelines, to secure U.S. ports of entry and coastline;
- The Services, National Guard, DHS agencies charged with securing borders and transportation, state governments, and infrastructure owners/operators to protect land borders and critical infrastructure nodes from attack;
- The Army Corps of Engineers, the National Guard, DHS Federal Emergency Management Agency (FEMA), and other relevant military operators (through NORTHCOM) to plan and practice for effective and timely emergency response and recovery;
- DARPA, DTRA, the Service R&D Labs, TSWG, DHS Science and Technology (S&T), DHS Domestic Nuclear Detection Office (DNDO) to create and execute coordinated Research, Development, Test, and Evaluation (RDT&E) agendas;
- DIA, CIA, NSA, NCTC, FBI, DHS IA and DHS S&T for better intelligence;

[8] See, for example, PDD 63, HSPD 17, and the National Infrastructure Protection Plan.

- OASD (HD)/DCIP, DHS (IP), DHS (S&T)and the key operations directorates at DHS for standardization of risk analysis methodologies;
- OASD (HD)/DCIP with support from DHS (IP) to enable and oversee the security of the Defense Industrial Base.

Providing clear roles and responsibilities for the two agencies and the mechanisms to assure coordination and integration should lead to cost savings through program reductions and/or elimination, as well as the creation of better capabilities for numerous agencies and users. For example, adaptation of DoD Force Protection and Anti Terrorism technologies and tools by DHS for use in homeland security applications could save the nation money and time to deploy. Coordination and collaboration at the RDT&E level could create improved risk analysis tools, security technologies, and risk mitigation capabilities for the nation's benefit. A partnership could also facilitate DHS pilots and test beds at DoD facilities and nearby infrastructure on which the facilities depend.

Recommendation: Institutionalize coordination and integration between DoD and DHS.

The Deputy Secretaries of DoD and DHS should direct that coordination and integration between the two departments be institutionalized through a formal Memorandum of Understanding (MOU) with a scope that includes the planning, research and development, acquisition, operations, and training contingencies that the two agencies will face together to secure the critical infrastructure of the homeland. The ASD (HD) in DoD and A/S (IP) in DHS should be assigned to implement the MOU, and the Deputy Secretaries should annually review progress.

B. DoD AND DEFENSE INDUSTRIAL BASE SECURITY

The nation's critical infrastructure is characterized by 17 sectors, with a federal department or agency lead assigned to ensure adequate steps for improving security are taken. This is a difficult task since much infrastructure is privately owned. DHS has the overarching role that includes establishing standards, providing guidance, developing a common knowledge base, and characterizing interdependencies among sectors. DoD is the Sector Specific Agency for the Defense Industrial Base (DIB).

DoD has broader responsibilities regarding infrastructure protection than just the DIB. Most comprehensively, DoD must address three classes of infrastructure and assets:

1. DoD-owned infrastructure and assets that support the National Military Strategy (e.g., DoD bases, installations, command and leadership centers);
2. Non-DoD infrastructure and assets that support the National Military Strategy (e.g., Contractor/Industry owned assets, especially the DIB and commercial infrastructure on which both #1 and the DIB depend);
3. Non-DoD infrastructure and assets that are so vital to the nation that their incapacitation, exploitation, or destruction could have a debilitating effect on the security or economic

well-being of the nation or could negatively affect national prestige, morale, and confidence.

The Defense Critical Infrastructure Program (DCIP) in OASD (HD) seeks to ensure that essential capabilities are available when the DoD needs them, and therefore, efforts focus primarily on the first two classes of infrastructure. The second class includes commercial infrastructure elements (power, water, telecommunications, etc.) and privately owned elements of the DIB. Both commercial infrastructure and DIB assets pose challenges that are not addressed in current protection activities directed toward DoD-owned and -operated assets. The third class is of interest to DoD should the President direct DoD to secure those sites, but the Task Force has focused on classes (1) and (2) consistent with its Terms of Reference.

With respect to commercial infrastructure, two major issues must be addressed. First, the interdependencies of commercial infrastructure elements that support critical DoD facilities are not yet entirely known. The DoD has the resident CIP expertise to assess these dependencies, but to date funding has only been available for a handful of assessments per year. Traditional (non-CIP) vulnerability assessments often do not assess vulnerabilities that reside "outside the fence," and do not address mission impact. A significant data collection and evaluation effort to fully establish a baseline for this facet of preparedness is needed.

Second, until recently, DoD had not established uniform policies and procedures to guide installation commanders in engaging with local providers to secure the infrastructure upon which the DoD relies.[9] To date, commercial infrastructure vulnerabilities affecting DoD installations have been identified in some cases, through state-wide and regional assessments, and in others, by enterprising installation commanders and like minded civil authorities. In addition, DoD supported site-specific vulnerability assessments have provided some information needed to take limited mitigation actions. While much of this interaction has been successful, greater uniformity would both aid installation commanders in their risk mitigation efforts and help ensure that DoD-wide security standards are understood and met.

With respect to the DIB, DoD must address three interrelated issues:

- In many cases, the DoD is not the primary customer. This has the potential to limit the degree to which the DoD can persuade DIB asset owners to incur additional costs by implementing new or improved security measures. From a business perspective, it may be preferable for a company to lose a DoD contract rather than comply with DoD security mandates.
- Even in cases where the DoD is the primary customer, business objectives may not be consistent with DoD security objectives. Businesses will seek to justify and recoup costs associated with improving security. The DoD should be prepared to address such costs as contracts surface for renewal.

[9] DoD Directive 3020.40, "Defense Critical Infrastructure Program," signed August 2005, assigns CIP responsibilities at all levels across the Department.

- Some critical DIB assets are located overseas. This severely limits the ability of the DoD to use regulatory mechanisms to ensure compliance with security guidelines, although threats to overseas DIB assets may be inherently greater and at higher risk than domestic DIB assets.

Recommendations: Take risk-based actions to improve DoD facility and DIB resiliency.[10]

To improve the security of DoD installations, the Task Force recommends the following actions:

- OASD (HD)/DCIP should oversee the characterization of the defense sector infrastructure dependencies, promulgate risk mitigation guidance, and establish uniform Defense Critical Infrastructure Protection (DCIP) standards;
- The Services should develop and implement plans to mitigate risk to an acceptable level and should provide an annual update of progress to the Deputy Secretary through the ASD (HD);
- Installation commanders should develop local assessments of infrastructure dependencies and implement risk mitigation plans consistent with guidance and standards;
- The Commander of NORTHCOM should integrate installation dependencies and infrastructure risk mitigation as a matter of command emphasis in his interaction with the Services in accordance with established OSD guidance and policy. Other Combatant Commanders should provide similar emphasis for DoD installations in their areas of responsibility.

To improve the security of the DIB, the Task Force recommends the following:

- OASD (HD)/DCIP should set policy objectives for managing the risks of critical DIB assets;
- USD (AT&L)/Office of Industrial Policy should review and revise, if necessary, Defense Federal Acquisition Regulations to ensure compliance with Policy objectives;
- Agencies, offices, and Service organizations in DoD with DIB critical links should review existing contracts of the critical DIB assets to ensure policy objectives can be addressed.

C. RISK-MANAGEMENT APPROACH TO DECISION MAKING FOR RESOURCE ALLOCATION

In order to effectively allocate resources, investment strategies should be embedded within a comprehensive risk management approach. Risk management is the sum of activities undertaken

[10] See Section III.C for a more specific discussion on risk assessment.

to understand, identify, classify, measure, and mitigate risk. The Task Force found that current resource allocation within DoD is not adequately matched to risk, significantly diminishing the overall effectiveness of the resources invested. The Task Force also found that under the current leadership at DHS, prioritizing allocation of resources consistent with risk is being emphasized, but methodologies for risk assessment are numerous and inconsistently applied.

A holistic risk management strategy implementation should address the following components:

- Threat assessment, both capability and intent;
- Vulnerability assessment;
- Consequence assessment;
- Mitigation options (cost/benefit) analysis; and
- Mitigation implementation.

The Risk Management process involves Risk Assessment (the combination of the first three risk elements – threat, vulnerability, and consequence) and Risk Mitigation (development and analysis of mitigation options and implementation of the preferred options). The first three risk elements are strongly interdependent for malevolent threats and must be considered collectively. The success of the Risk Assessment process depends strongly upon good planning, a screening process based upon a preliminary analysis of consequences, and the development of a good baseline description (from which the mitigation options can be developed). The output of the Risk Assessment provides the degree of risk that is to be managed. Various mitigation options can then be analyzed in a holistic context that considers other operational parameters such as life-cycle cost, operational impact, safety, policy, public opinion, and personal freedoms. These options provide input to the next round of risk assessments that result in risk/operational pairs. For each option there is a reduction in risk and an associated operational "cost" – a real cost (e.g., life-cycle security, productivity, safety), and a virtual cost (e.g., public opinion, loss of personal freedoms). Only then does the decision-maker have the necessary data to determine which risks should be mitigated and which risks should be accepted.

Furthermore, all involved in the process must understand the perishability of any risk assessment. With time, all factors can change: the threat may become more or less capable or "threatening"; vulnerabilities can become more pronounced or less so (because of the implementation of mitigation options, or lack thereof); and consequences may be higher or lower depending on intervening developments involving the asset in question or related assets that can may or may not be robust substitutes should something happen to the asset in question. As such, commitment to a risk management strategy also carries a commitment to a continuing process.

In the Task Force's evaluation of the differing assessment methodologies being deployed within DoD under the banner of "infrastructure" or "facility/base" protection, the Task Force observed that current methodologies are too heavily focused on vulnerability assessment, are based upon compliance rather than performance, and do not adequately address the important components of threat assessment, consequence assessment and mitigation options analysis. While it is important to engage in vulnerability assessments, focusing solely within the vulnerability domain

does not provide an appropriate context for the evaluation of risk and the effective allocation of resources. In conducting vulnerability assessments, a proper balance should be obtained between performance measures and compliance standards; meeting performance criteria is generally preferable, especially for critical assets.

In addition, the Task Force learned that over two dozen competing vulnerability assessment methodologies are being variously applied throughout DoD. Many of them appear to be duplicative and nearly all of them have diminished effectiveness due to the lack of integration of the results within an overarching risk management approach. In most instances, the Task Force could identify no link between assessment results and resource allocation. This is not surprising as the failure to provide appropriate threat, consequence, and mitigation analysis results in the vulnerability assessment lacking appropriate decision-making context.

The situation at DoD is further complicated by a tendency to add programs and activities motivated by specific events, threats or concerns (e.g., AT/FP, CIP, COOP, CBRNE, cyber, Project Guardian, etc) on top of the more traditional installation preparedness responsibilities of the base/installation commander. Each program is stood up with its own program office and administered through separate parts of the Department. The plethora of separate assessments coupled with the growth of distinct protection programs leads to needless confusion among base and installation commanders in setting priorities for continuous improvement of the security posture of the facilities for which they are responsible. It should be evident that the Department is much better served through a coordinated and integrated effort to address a wide range of threats with a single risk mitigation strategy.

Recommendation: Assign leadership for integrated risk management and mitigation at DoD.

The Task Force recommends that the DEPSECDEF designate a lead agency or office for an integrated risk management and mitigation program with responsibilities to:

- Consolidate the many vulnerability assessment programs into one risk assessment program that includes performance based criteria, and considers the spectrum of current and future threats;
- Seek congruence of methodologies and tools with DHS (IP) and avoid duplication of effort;
- Help identify prudent risk mitigation measures and assess progress in achieving improved levels of security;
- Ensure deployment in a nested fashion from "global" to local;
- Evaluate resource allocation by infrastructure owners (both within DoD and the DIB) for consistency with risk assessments; and
- Assure timely cycling back through the process as conditions change.

This risk management program should establish a capability to match risk mitigation resources to risk at all levels and provide flexibility for the assessed organization to make risk mitigation

decisions at the local level of the base or installation commander. Included should be the degree to which each commander needs to adopt the guidance and/or capabilities proffered by the several security improvement programs of the Department. ASD (HD)'s proposal for achieving mission assurance[11] should be considered for addressing these issues.

D. UNDERSTANDING INFRASTRUCTURE INTERDEPENDENCIES

While it is a common assumption that reliance on critical infrastructures is increasing and that those infrastructures are inherently vulnerable, DHS and infrastructure owners have only a limited understanding of the interdependencies that exist among and between the infrastructure sectors. In order to adequately assess the consequences of infrastructure attacks, DHS requires more robust tools to catalog the complex infrastructure interdependencies and model the cascading consequences of infrastructure failures. The National Infrastructure Simulation and Analysis Center (NISAC) funded by DHS (IP), and a small program in DHS (S&T), called CIP/Decision Support System (DSS), are aimed in this direction but at current funding levels, will take a number of years to create a comprehensive capability.

Even with a "national" set of tools and data, DHS must also create effective mechanisms to share the information with infrastructure owners/operators, who should, in turn, engage in risk management to determine appropriate levels of protection. While there are many information-sharing initiatives that have been put in place over the past decade, they are too heavily focused on sharing vulnerability information, leaving users of the information at a loss for understanding threat, consequences, and the trades among mitigation options. (In addition, many of the initiatives have so poorly protected the information provided that infrastructure owner or operators have become reluctant to share new and/or updated information with the federal government. The Task Force elaborates on this point in Section H.)

Recommendation: Accelerate the shared understanding of infrastructure interdependencies.

The Task Force recommends that:

- DHS (S&T and IP) accelerate characterization of infrastructure interdependencies and fold the results into analytical tools that can be used by sector owners, so that they can assess and implement mitigation measures to avoid sector failures due to the failures of a different sector;
- DHS (IP) implement protected information sharing methods that could accelerate mitigation planning at the local level; and
- DoD through OASD (HD)/DCIP seek priority for both of the above with DHS through an MOU with DHS; the MOU should address areas for collaboration to enhance understanding of infrastructure dependencies and establish a coordination mechanism for the development of tools to assess interdependencies and model cascading failures.

[11] "Strategy for Homeland Defense and Civil Support," signed June 2005.

E. BEST PRACTICES

Given the enormity and complexity of the nation's Critical Infrastructure, the task of identifying "best" practices proved impossible. The Task Force instead sought out examples of exemplary practices through briefings and field trips based on the collective knowledge of Task Force members, government advisors, and private sector contacts. Sources of these exemplary practices came from government and business alike.

Interoperability and Integration: New York City and Environs. New York City continues to operate under a "High" terrorism threat level. As a consequence, the city government, transit authorities and surrounding enterprises have developed a rich set of exemplary practices through continual operations and exercises. For example, the New York City Police Department exercises effective communication with private sector security directors responsible for critical infrastructure and protection of the city's business sector through an e-mail and briefing program named the Area Police and Private Sector Liaison (APPL). The APPL unit is part of the Chief of Police's office and issues around-the-clock updates of current threat information. It also shares information on improving security procedures; major crimes such as bank robberies; major events such as the 2004 Republican National Convention or the convening of the UN General Assembly; major sporting events; authorized flyovers; and traffic and transportation disruptions. This healthy communication not only improves security practices within the business community, but also suppresses anxiety by enabling security directors to inform employee populations of events impacting their daily work environment.

The Office of Emergency Management in New York City has also developed examples of good practices. They have created a state-of-the-art communications and operations center with representation from every organization that might be involved in a major event impacting the city. Their broad focus encompasses natural disasters, fires, power outages, etc., as well as terrorist related attacks. Their primary role is to coordinate city assets in response to major events. They maintain an active database of resources that are available not only within the city government, but also private assets that might be needed in a disaster (e.g., heavy construction equipment, cranes, ships, barrages, high tech equipment, laboratory analysis locations, medical specialists, etc.). The database is updated quarterly. They have also supported the formation of trained Community Emergency Response Teams (CERTs) and have pre-credentialed key personnel from the private sector to engage if needed.

The Metropolitan Transit Authority (MTA) has done a comprehensive risk assessment of the various modes and nodes (buses, subways, trains, airplanes, terminals) within its area of responsibility. It has developed and/or improved a number of specialized or existing capabilities as a result (e.g., the Emergency Service Unit expanded its capabilities to include HAZMAT capabilities). MTA believes that one of its most effective efforts has been the education and involvement of both employees and customers in the "see something, say something" campaign.

Naval Militia: An Underutilized Resource?

New York Naval militia represents a unique example of the Federal Government providing immediate access to Navy and Marine reservists during State and Local emergencies, at no cost to DoD. It is an all volunteer force of active (95% or more of the members must be Title 10 active reservists in order for a Naval Militia to be Federally recognized) and retired reservists who are called to State active duty in the same way Army and Air National Guard members are mobilized. Once mobilized, Naval Militia personnel are employed in joint operations under the command of the State Adjutant General until Federal mobilization, should the need arise.

Naval Militias date back to the colonial era, and were the Navy's principal source of reserve manpower until WWII. They once existed in every maritime state, but few remain today. New York State operates the most active and largest of the remaining Naval Militias, with a current membership level of about 4,500 personnel. While conventional wisdom may question the need for naval forces responsive to a governor on short notice, experience demonstrates that Naval land forces such as the Sea Bees play critical roles in disaster recovery operations. However, as important as that contribution continues to be, the Naval Militia capability in highest demand today is protection of our port and waterway critical infrastructure.

The New York–New Jersey harbor system is vulnerable and subject to risks that exceed the Coast Guard's ability to mitigate. Recognizing its resource limitation, the Coast Guard has teamed with the NY Naval Militia and harbor pilots to conduct joint security operations. Naval Militia boats and crews, operating in State status under Coast Guard direction, conducted 13,729 harbor and river security patrols in the first three years of the post-9/11 port security mission. Replicating this success story in many other states will allow tens of thousands of DoD trained military personnel to participate in the protection of DoD and DIB critical infrastructure on a regular basis, without interrupting Navy or Marine Reserve training necessary to perform the federal mission.

Military-Civilian Collaboration: Norfolk. A visit to the Norfolk Naval Base revealed a maturing and comprehensive relationship with the City of Norfolk. This contrasts with a visit by one of the Task Force members 2 years earlier (when the Navy was just standing up consolidated regional planning and operations under the Chief of Naval Installations), in which the relationships extended only to mutual aid agreements. Security operations planning reflected a strong working relationship between the principals at the Naval Station and city leaders in the public health, police, fire and rescue, and information technology departments. They were training and exercising with regularity, working to improve communications interoperability, and developing joint plans for emergency response. While not as mature as the partnership between Camp LeJeune and Oslo County, the City of Norfolk-Navy ties can be cited as one of mutual respect, a drive for improved understanding and capabilities, and agreement on priorities for protection and security. Both military and civilian representatives felt, however, that they were largely on their own to develop solutions and to "scratch" for funds. The military felt they were getting equipment that they did not regard as highest priority (e.g., through the Guardian Program), while the civilians cited the difficulties in getting both guidance and grants from DHS.

Industry Standards: Chemical Sector. The chemical industry offered two examples worthy of mention. First, the American Chemical Council (ACC), the industry association, used member resources to develop a formal process for identifying critical assets requiring protection. They then developed a manual providing guidance for the development of a security plan for facilities and critical assets. These products for identification of critical assets and security guidance were made available to not only the membership of the ACC but to the entire business sector through their Information Sharing and Analysis Center.[12]

The second example came from Pittsburgh Plate Glass (PPG), where the general principles of the ACC have been put into practice. PPG implemented a program across all its facilities that prioritized the hazardous chemicals on-site for off-site impact in the event of an unintentional or terrorist initiated release, and then modeled the off-site consequences. This led to the establishment of priorities and the implementation of both security and response measures to mitigate against adverse impacts from any sort of unplanned release. PPG also installed interactive surveillance technology along the waterside areas of their facilities to identify potential waterborne threats. This is an example where technology contributed to better security and quicker response while saving personnel necessary to monitor the waterfront.

Intra-sector Cooperation: Financial Sector. An informal Financial Services Coordination Committee established by the Bankers and Brokers security directors in New York City has developed into an important body to aid in decisions on how to analyze threat information, organize requests for governmental response and determine how to best protect key assets of their institutions. Regular conference calls during high threat periods ensure the distribution of key information from government authorities and a quick coordinated response by the entire financial sector.

Public/private Cooperation: Telecommunications Sector. BellSouth's work with the National Security Telecommunications Advisory Council (NSTAC) highlighted how private sector infrastructure is critical to the nation and how cooperative efforts can pay dividends. The NSTAC established a senior level Business Continuity and Security Committee to oversee corporate security in the tracking of incidents and efforts to prevent incidents. The committee also developed protocols for security incident response, business continuity and disaster recovery. The industry has built networks designed to survive natural or malevolent events through the utilization of redundancy, self-repairing fiber, emergency power and portable generators, when needed.

Comprehensive Risk Assessment and Mitigation: Bonneville Power Administration. Leadership at this utility recognized in 1997 that they could not afford to protect their entire system, so they recruited appropriate external technical help and put into practice one of the most comprehensive risk assessment and mitigation plans that the Task Force discovered. They were a key player in the formation of the Interagency Forum on Infrastructure Protection (IFIP), which sponsored the development of the Risk Assessment Methodology for Dams (RAM-D) published in August

[12] The industry has been historically focused on safety – establishing standards and sharing best practices. They are approaching security in a similar manner, although some in Congress believe that they are not moving fast enough and have stepped in with federally mandated requirements in the time period since the Task Force was briefed by the ACC.

2001, and a follow-on version for electric transmission, RAM-T. As an example of a shift in resources based upon these methodologies, they had spent $2.7M in protective force services spread across the entire system pre-9/11; they significantly increased and concentrated those expenditures post-9/11 to several key dams while also shifting to remote monitoring and control of dispersed substations. They have applied RAM-D and RAM-T at their important facilities and have demonstrated to their executive leadership that their mitigation strategies are effective in reducing risk while minimizing operational impact. They have also been successful in ensuring leadership participation in major exercises, which have been aimed at understanding interdependencies of the system with other sectors and vice versa.

Development and Application of Tools and Technologies: Department of Energy and the Nuclear Regulatory Commission. DOE has created a set of performance-based measures for the highest valued nuclear assets and reduced measures for lower value assets while still requiring compliance with a minimum standard. To support assessments, DOE has invested, principally through the national labs, in the development and application of a suite of modeling tools and supported extensive analyses to evaluate the use of alternative security measures and procedures. They have a history of nurturing the advancement of security technologies through a long standing research and development program; many of these technologies have been transferred to industry. The Nuclear Regulatory Commission is a working partner with DOE in the maturing and application of the assessment tool kit. Many of the current tools being used had their origins in the NRC safety assessment program.

Technology to improve security (DIB): Northrop Grumman. This company provided one of the few examples where technology has been used to offset manpower. Its security program leadership has consolidated command post facility monitoring into a single site for all its US assets. A secure information network facilitates both real time monitoring and the alert function back to the site should an incident occur.

Recommendation: Create a brokering function through the Government Coordinating Committees and Sector Coordinating Committees to promulgate "Best Practices."

The Task Force observes and recommends that:

- DHS (IP) should monitor, collect, and share best practices for all sectors, but especially for owners of critical facilities or nodes. The DHS (IP) role is clear in this recommendation. Resources need to be devoted to the search for practices that best protect the nation's critical infrastructure upon which our military, businesses and the public are dependent. Once vetted for universal applicability, sharing and high-visibility become the task at hand. The DHS Government Coordinating Councils (GCC) and Sector Coordinating Councils (SCC) will play a pivotal role in all aspects of best practices. They will facilitate information sharing, assessment of good and best practices, and the establishment of standards and guidance to be promulgated throughout the private sector and government agencies.

- DoD can both benefit and contribute to this effort. However, DoD does not have a structure for coordinating the implementation of best practices. In the interest of

protecting U.S. military readiness and capabilities, DoD should establish through OASD (HD)/DCIP a process that incorporates the identification, communication, and implementation of best practices as part of the previously recommended risk management and mitigation program.

F. SYSTEMS AND TECHNOLOGIES

To date, the potential of technology to enhance security of DoD facilities and infrastructure is far from being fully realized. The primary use of technology is for physical security and surveillance of facilities and infrastructure. This includes physical barriers, electronic surveillance, ID badges, etc. While these applications improve security, they have not been exploited to a level that allows significant reductions in manpower. Similar to the experience in the software/computer revolution, one should expect a delay between the introduction of technology to improve capability and the leveraging of manpower. In fact, manpower requirements will likely change but not necessarily decline initially – as technology is introduced, it often requires new and higher skill sets to maintain and exploit it. Therefore, the Task Force believes technology development, which should ultimately reduce manpower requirements for infrastructure security, is an appropriate goal, but to date little creativity and scant resources have been applied to developing new and unique capabilities to deliver such a benefit.

There are many opportunities for common support system and technology needs between DHS and DoD. DoD areas where systems capabilities are common to DHS applications include urban and counter insurgency operations, non-lethal weapons, wireless communication, distributed ground sensor arrays and other surveillance techniques, intelligence data mining, etc. However, there is no designated owner for Homeland-Security related technology in DoD. Of even greater concern is that there is strong direction from DARPA leadership to avoid participating in such areas, including contributing to this study. This is all the more troublesome given that a number of "Grand Challenges" cannot be addressed without some dedicated R&D efforts by top talent. Examples include:

- Detection of surveillance activities;
- Stand-off detection of chemical, biological, nuclear, radiation and explosive hazards;
- Monitoring "people of interest" while protecting civil liberties;
- Detection of hostile intent;
- Detect & deny airborne threats; and
- Detect & deny waterborne threats.

Recommendation: Establish a vigorous R&D program to address the "Grand Challenges" of infrastructure protection.

The Task Force recommends that the ASD (HD) and USD (AT&L) designate DDR&E to develop a joint R&D program with DHS (S&T). Such a program should address and fund the "Grand Challenges," whose solutions will require top teams from academia, government, and industry. In addition, this interagency program should support the adaptation of useful technologies from other military areas to Homeland Security. DoD and DHS must also support deployment of security systems and technology. This requires:

- Integration of modeling and simulation tools;
- Use of pilots to experiment with and refine new systems and technologies;
- Development of CONOPS for Homeland Security applications; and
- Training of operators in the field prior to systems deployment.

As the "technically tolerant" first user, DoD should be willing to provide sites for piloting new systems and technologies.

G. STANDARDS AND METRICS

A number of groups at DHS and DoD have roles that contribute to establishing standards and metrics, but they tend not to be integrated and as a result, a comprehensive program does not yet exist. Among the players:

- DHS (S&T): The directorate has established a Standards Program with the responsibility to develop and coordinate the adoption of national standards and appropriate evaluation methods for equipment marketed to meet homeland security mission needs. The scope includes identification of requirements and prioritization of needs; development and adoption of standards and guidance through a community consensus process; development of metrics and protocols for component and system test and evaluation; and coordination of standards development between U.S. and international partners.

- DOC NIST: DHS has enlisted NIST to support its Standards Program.

- Interagency Committee on Standards Policy (ICSP): ICSP advises the Secretary of Commerce and other Executive Branch agencies in standards policy matters. The Committee reports to the Secretary of Commerce through the Director of the National Institute of Standards and Technology (NIST).

- DoD Physical Security Equipment Action Group (PSEAG): The PSEAG identifies and prioritizes the Services' needs for new physical security equipment, and funds the development of the highest priorities.

- OASD (HD)/DCIP: Engages DHS (S&T) Standards Program as resources allow.

DoD has yet to position itself to influence DHS, NIST, or the interagency committee by promulgating objectives and standards for securing critical assets. At the same time, the pieces in these other agencies do not make for a comprehensive program, which should include:

- Policies, practices, and procedures (e.g., risk analysis, compatibility and interoperability, training, test and evaluation, integration with existing concepts of operation, lifecycle costs); and
- Materiel and system requirements and measures of effectiveness (e.g., CBRNE detection and decontamination, personal protective equipment, biometric identification, cyber protection).

Recommendation: Support common standards and metrics.

The Task Force recommends that:

- OASD (HD)/DCIP articulate clear DCIP objectives and develop standards and benchmarks for identifying and assessing DoD dependencies on critical infrastructure;
- OASD (HD)/DCIP work with ASD (SO/LIC) and USD (I) (through the Defense Security Agency) to promulgate standards for mitigating risks of critical assets both at home and abroad;
- OASD (HD)/CIP engage the DHS Standards Program regarding CIP tools, components, systems;
- OASD (HD)/DCIP, in consolidating risk assessment tools, in particular, should coordinate with the DHS effort with ASME RAMCAP to ensure a standardized approach for such assessments.

H. INFORMATION SHARING

The most significant challenge to working with both commercial infrastructure providers and DIB asset owners is the establishment of legal provisions to support the protection of sensitive information related to infrastructure sector private operations. While critical infrastructure information provided to DHS is protected by the Protection of Critical Infrastructure Information (PCII) program, the DoD must obtain statutory authority and must establish appropriate policies to govern the protection of sensitive information. Some specific issues the DoD must address include:

- Exemption of proprietary and other unclassified sensitive information from the Freedom of Information Act (FOIA);
- Impact on companies the DoD identifies as owning critical assets;
- Liability from inadequate correction of vulnerabilities or for failure to reasonably defend or plan against threat occurrences;
- Forced information release as a consequence of discovery; and

- Protection of proprietary or other sensitive information.

To address the shortcoming in information sharing with private infrastructure owners/operators, DHS (IP) must take the lead to develop mechanisms for protection and sharing information on infrastructure operations and dependencies. A particularly thorny issue is the lack of classification guidance from DHS. DHS currently relies on the classification guidance of other agencies (DoD and DOE, in particular). In addition, the "sensitive but unclassified" category of information for DHS requires careful review and implementation of the proposed Sensitive Homeland Security Information since it will be the official interface to state, local, tribal, and some private sector entities. The PCII mechanism helps cover part of the issue, but it continues to be problematic with private industry and may need significant revision to be effective. Certainly the issue of how much information the Federal Government really needs for effective homeland security, how to protect that information, and how to share it appropriately, were all open questions at the time this Task Force concluded.

Recommendation: Place high priority on resolving information sharing and information protection issues.

DHS must develop and implement a complete set of classification guides including information that is unclassified but sensitive. In addition to legal and policy analysts, subject matter experts should assist in the development of these guidelines. For those categories involving information that will be shared with non-Federal and non-Government entities and protected by them, development of the guidance with representatives of those entities is recommended.

In accordance with applicable laws or regulations, ASD (HD) and other DoD components should collaborate with appropriate private-sector entities and continue to encourage the development of information sharing and analysis mechanisms. Additionally, the DoD and other federal agencies must collaborate with the private sector and continue to support interdependency analysis mechanisms.

I. CONCLUSION

The country's security programs have come a long way since the events of September 11, 2001; however, they still have a long way to go to achieve a level of satisfactory risk management and mitigation for the nation's infrastructure. The Task Force sees the possibility of providing the necessary security and protection, starting with effective management and coordination at the Federal level. In this report, the Task Force has highlighted opportunities for both improved management and focused investment to achieve those goals.

The Task Force would like to add that as this study was performed on protecting critical infrastructure as outlined in the Terms of Reference and viewed in the Department, it became obvious that a much bigger issue lies outside the protection of DoD critical facilities alone. A starting focus should be in the area of protection of the country and its military national security mission capability. This study was staffed and focused on the classical protection of critical facilities. Military strategy, policy, doctrine and planning can have much more significant

impact on protecting critical mission capability by looking at the distribution of assets; e.g., positioning of fighter wings in lower concentrations and at less vulnerable facilities than for example, Langley; or naval ship basing in multiple ports, thereby reducing the concentration in Norfolk and San Diego. As for depending on the private sector, including the defense industrial base, the same principal applies – namely policy and strategy, which limit the concentration of critical assets that can protect mission capability much more than facility protection alone. This study has recommended reasonable beliefs in protecting critical military facilities, including the defense industrial base. A second view would consider policies and strategies for making facilities less critical rather than just protecting critical facilities. The Task Force recommends that the Secretary of Defense direct the staffing of such a study with the capability to look at the issue in this new light.

A. TERMS OF REFERENCE

THE UNDER SECRETARY OF DEFENSE

3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

JAN 20 2004

ACQUISITION, TECHNOLOGY AND LOGISTICS

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT Terms of Reference—Defense Science Board Task Force on Critical Homeland Infrastructure Protection

You are requested to establish a Defense Science Board (DSB) Task Force to assess best practices for protecting US homeland installations and recommending various approaches to enhancing security and protection of these facilities.

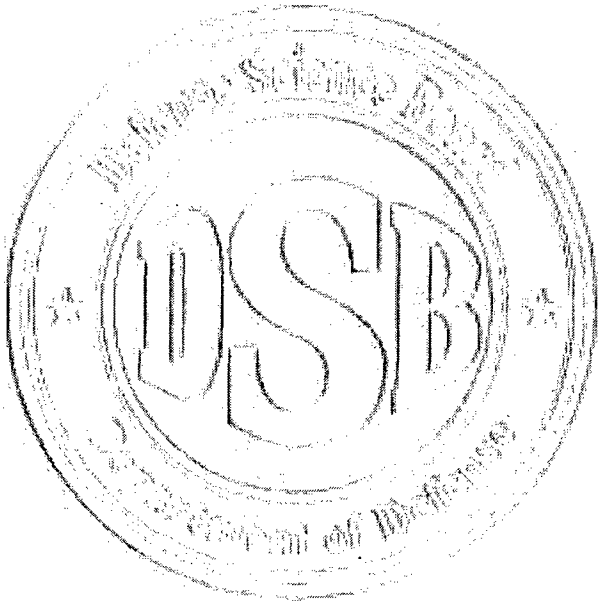
With the increased emphasis on the need for improvements to US homeland security measures, investments in technology and manpower should be considered in order to ensure proper security levels at our nation's high-value installations with particular emphasis on airports, harbors, nuclear power facilities and military bases. To that end, the Task Force should

a) review existing best practices, to include risk management approaches, in force protection and security at civil, industrial and military complexes
b) assess shortfalls and deficiencies associated with operational security
c) identify promising technology and/or processes that will enhance security
d) recommend methods for reducing overall manpower requirements without relinquishing robust security measures
e) identify issues and offer recommendations for the balance between military and private responsibilities for critical facility protection
f) understand security standards and metrics and identify any gaps

The study will be co-sponsored by me as the Acting Under Secretary of Defense (Acquisition, Technology and Logistics), Assistant Secretary of Defense (Homeland Defense) and by the Department of Homeland Security. Dr. Ron Kerber and Dr. Miriam John will serve as the Task Force Co-Chairs. Mr. William Bryan, OASD(HD) will serve as Executive Secretary. LtCol David Robertson, USAF, will serve as the Defense Science Board Secretariat representative.

The Task Force will operate in accordance with the provisions of P.L. 92-463, the "Federal Advisory Committee Act," and DOD Directive 5105.4, the "DoD Federal Advisory Committee Management Program," It is not anticipated that this Task Force will need to go into any "particular matters" within the meaning of Section 208 of Title 18, U.S. Code, nor will it cause any member to be placed in the position of acting as a procurement official.

Michael W. Wynne
Acting


DSB

B. TASK FORCE MEMBERSHIP

Task Force Chairpersons

Dr. Miriam John, Chair, *Sandia National Laboratories*

Dr. Ronald Kerber, *Private Consultant*

Executive Secretary

Mr. William Bryan, Director, *Critical Infrastructure Protection*

Task Force Members

Mr. Gregorie Bujac, *Altria Corp. Services*

Dr. John Cummings, *DHS S&T*

Mr. Matthew Devost, *Terrorism Research Center*

MG (ret) John Fenimore, *Private Consultant*

Dr. Barry Horowitz, *University of Virginia*

Dr. Dennis Miyoshi, *Sandia National Laboratories*

Mr. Winston Wiley, *Booz Allen Hamilton*

Government Advisors

LTC Kelvin Bright, *Joint Staff*

Dr. Bradley Clark, *DHS*

Mr. Wade Ishimoto, *OSD*

Mr. Bert Tussing, *Army War College*

Mr. Larry Wheeler, *DHS*

DSB Secretariat

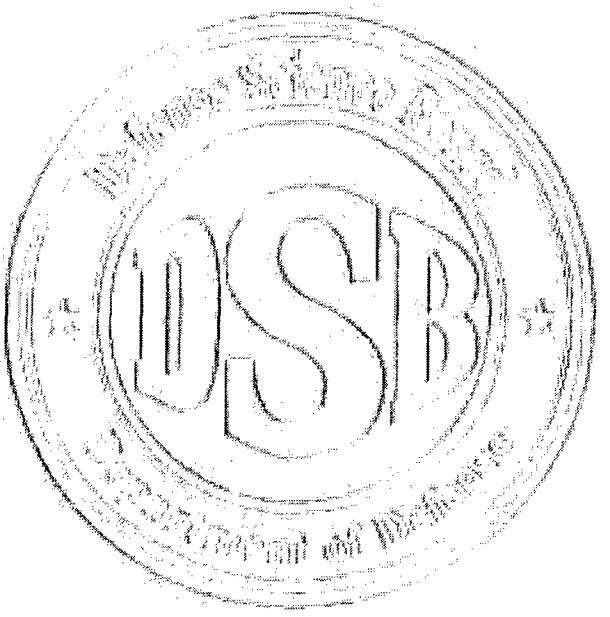
LtCol David Robertson, USAF, *Defense Science Board*

Maj Charles Lominac, USAF, *Defense Science Board*

Support

Ms. Anne Buckingham, *NSR Inc.*

Ms. Diana Conty, *SAIC*


DSB

C. BRIEFINGS RECEIVED

20 – 21 Jan. 2004

Remarks on Homeland Defense	Hon. Paul McHale	ASD(HD)
Review of DSB Summer Study: DoD Roles and Missions in Homeland Security	Mr. Don Latham	General Dynamics
DSB Legal Considerations		DoD General Council
DoD Critical Infrastructure Protection (CIP) Program Overview	Mr. William Bryan	OASD(HD)
Threats to Defense Critical Infrastructure	Dr. Richard Gault	DIA
Defense Program Officer for Mission Assurance (DPO-MA) Overview	Mr. John Keenan	DPO-MA
The Defense Industrial Base (DIB)	Mr. Bill Ennis	DCMA
Operationalizing CIP	Mr. Dan Mathis	DPO-MA
The National Innovative Technology and Mission Assurance Center	Ms. Elizabeth D'Andrea	NITMAC
Current and Developing Issues in Applying CIP to the DIB	Mr. Mike Berry	DSS
OPSEC Overview	Mr. Garry Manning	IOSS

26 – 27 Feb. 2004

OSD CIP Update	Mr. William Bryan	OASD(HD)
DHS CIP Science and Technologies activities and plans	Dr. John Hoyt	DHS
Current CIP Threats	Mr. James Woolsey	
Applied Risk Management – Physical Security Assessments	Mr. Dan O'Neill	ARM
DHS – Introduction to IA, IP, CIAO, NIPC, and NIST	Mr. Larry Wheeler	DHS
BellSouth – Infrastructure Protection and Business Continuity	Mr. David Barron	BellSouth
SAIC – SAIC's Approach to Infrastructure Controls	Mr. Steve Lines	SAIC

Northrop Grumman – Physical Security; Best Practices in Support of DoD Contracts	Mr. Greg Swain, Ms. Patricia Tomaselli, Mr. Tony Ingenito	Northrop Grumman
National Industrial Security Program	Ms. Rosalind Baybutt	OSD-USDI

30 – 31 Mar. 2004

FSIVA Process	LTC John Lazaro	Joint Staff
Site Survey	Mr. Michael Shanahan	DPO-MA
DOE's Transition from a Prescriptive Security Approach to a Risk Management System	Mr. Samuel Callahan	DOE
Terrorist Threat Intelligence Center Overview	Mr. John Brennan	TTIC
BSA Overview and Site Assessment	Mr. David Lewis	DTRA
Computer Network Vulnerabilities and Countermeasures	COL Jeff Brown	JTF-CNO
Telecommunications Security and NSTAC	Mr. Karl Rauscher	NSTAC
Anti-Terrorism/Force Protection	LTC(P) Charles Tennison	SO/LIC
Physical Security at Chemical Sites	Ms. Dorothy Kellogg	American Chemistry Council

10 – 11 May 2004

Emergency Response Technology	Mr. David Drescher	Roam Secure
National Guard Bureau	COL Peter Aylward	NGB
Technical Support Working Group Infrastructure Protection Technologies	Mr. Perry Pederson	TSWG
Cyber Security in the Financial Arena	Mr. Jay Healey	White House Homeland Security Council
Physical Security Equipment Action Group	Mr. Lamar Young	PSEAG
Amalgam Virgo 04/Determined Promise 04	LTC Kelvin Bright	Joint Staff

23 – 24 June 2004		
Regional Security Coordination	CAPT Shawn Morrissey	Navy
Mid-Atlantic Regional Security	CDR Herb Jansen	Navy
Anti-Terrorism	Mr. Tim Atwell	ATO NS Norfolk
WMD Five Major Cities Exercise Results	Maj Scott Kunkel	(USAF) JFCOM
City of Norfolk Emergency Operations Center	Mr. Ron Keys Mr. Bruce Marquis	Norfolk Emergency Operations /Center Norfolk Police Department
Newport News Shipping Overview/Security Overview	Mr. Derek Jenkins	NNSY
Langley AFB Security Issues and Operations	Mr. Stan Huddleston	Air Force

20 – 21 July 2004		
DHS IAIP Organization/Standards and Metrics	Ms. Pamela Greenlaw	DHS
DOE Physical Security Research and Development	Mr. Carl Pocratsky	DOE
CBRN Installation Protection Program	COL Camille Nichols	Joint Project Manager Guardian
DARPA Overview	Mr. Roger Gibbs	DARPA
LLNL Technologies in Support of Infrastructure Protection	Mr. Don Prosnitz	LLNL
Sandia National Laboratories S&T Capabilities for CIP	Dr. Miriam John	Sandia National Laboratories
DHS S&T Countermeasures/Project Safe Commerce	Ms. Huban Gowadia	DHS

26 – 27 Aug. 2004		
Northern Command (NORTHCOM) Critical Infrastructure Protection (CIP) Strategic Plan	Mr. Patrick Paulsen	NORTHCOM
PPG Security Overview	Mr. Regis Becker	PPG
Bonneville Power Association (BPA) Security and Emergency Management	Mr. Robert Windus	BPA
Overview of NRC Security Activities	Mr. Glenn Tracy	NRC
NISAC Overview	Mr. Jon Larsen	NISAC
Association of Metropolitan Water Agencies (AMWA) Water Security	Ms. Erica Brown	AMWA
ASME Risk Analysis and Management for Critical Analysis Protection (RAMCAP) Program	Dr. Robert Nickell	ASME
DHS Control System Security	Mr. David Sanders	DHS
4 – 5 Oct. 2004		
Nuclear Security/Post-9/11 and Security Measures at Indian Point Energy Center	Mr. Jim Knubel	Entergy
Office of Emergency Management – New York City	Mr. Paul Katzer, Mr. Robert Wilson	OEM-NYC
Securing NY Metropolitan Transit Authority's Rail System	Mr. William Morange	NY-MTA
Terrorism Threat Level/NYPD Response and Preparedness	Mr. Phil Pulaski	NYPD Bureau of Counterterrorism
Coast Guard Security	CAPT Scot Graham	Coast Guard
Security Issues within the Board of Commissioners of Pilots of the State of New York	Commissioner Robert Pouch	Board of Commissioners of Pilots of the State of New York
28 – 29 Oct. 2004		
NORAD Air Defense Vulnerabilities	LTC Randy Morris	Air Force
23 Feb. 2005		
CSIS Briefing	Ms. Anne Witkowsky; Mr. David Heyman	CSIS

D. ACRONYMS

ACC	American Chemistry Council
AOR	Area of Responsibility
APPL	Area Police and Private Sector Liason
A/S	Assistant Secretary
ASD	Assistant Secretary of Defense
ASD CIP	Assistant Secretary of Defense, Critical Infrastructure Protection
ASD HD/CIP	Assistant Secretary of Defense, Homeland Defense/Critical Infrastructure Protection
ASD SO/LIC	Assistant Secretary of Defense, Special Operations/Low Intensity Conflict
ASME	American Society of Mechanical Engineers
AT/FP	Antiterrorism/Force Protection
CBRNE	Chemical Biological Radiological Nuclear Explosive
CERT	Commuter Emergency Response Team
CIA	Central Intelligence Agency
CIP	Critical Infrastructure Program
COCOM	Combatant Command
CONOPS	Concept of Operations
CTC	Counter Terrorism Center
DARPA	Defense Advanced Research Projects Agency
DCIP	Defense Critical Infrastructure Program
DDRE	Director of Defense Research and Engineering
DEPSECDEF	Deputy Secretary of Defense
DFAR	Defense Federal Acquisition Regulation
DHS	Department of Homeland Security
DHS S&T	Department of Homeland Security, Science and Technology
DHS IP	Department of Homeland Security, Infrastructure Protection
DHS IA	Department of Homeland Security, Information Analysis
DHS PREP	Department of Homeland Security, Directorate for Preparedness
DIA	Defense Intelligence Agency

DIB	Defense Industrial Base
DNDO	Domestic Nuclear Detection Office
DOC	Department of Commerce
DoD	Department of Defense
DOE	Department of Energy
DSB	Defense Science Board
DSS	Defense Security Service
DTRA	Defense Threat Reduction Agency
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FOIA	Freedom of Information Act
GCC	Government Coordinating Council
GOCO	Government Owned, Contractor Operated
HAZMAT	Hazardous Material
HD	Homeland Defense
HD/CIP	Homeland Defense/Critical Infrastructure Protection
HS	Homeland Security
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MTA	Metropolitan Transit Authority
NIST	National Institute of Standards and Technology
NORTHCOM	US Northern Command
NSA	National Security Agency
OASD(HD)	Office of the Assistant Secretary of Defense for Homeland Defense
ODP	Office for Domestic Preparedness
OSD	Office of the Secretary of Defense
OSD/CIP	Office of the Secretary of Defense/Critical Infrastructure Program
OUSD(AT&L)	Office of the Under Secretary of Defense for Acquisition, Technology and Logistics
PCII	Protection of Critical Infrastructure Information
PPG	Pittsburgh Plate Glass
PSEAG	Physical Security Equipment Action Group

RAMCAP	Risk Analysis and Management for Critical Asset Protection
R&D	Research and Development
RDT&E	Research, Development, Test and Evaluation
SCC	Sector Coordinating Council
TSA	Transportation Security Administration
TSWG	Technical Support Working Group
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
UN	United Nations
US	United States