

~~FOR OFFICIAL USE ONLY~~

Report No. DODIG-2012-064

March 13, 2012

Inspector General

United States
Department *of* Defense



Vulnerability and Risk Assessments Needed to
Protect Defense Industrial Base Critical Assets

~~FOR OFFICIAL USE ONLY~~

Additional Copies

To obtain additional copies of this report, visit the Web site of the Department of Defense Inspector General at <http://www.dodig.mil/audit/reports> or contact the Secondary Reports Distribution Unit at (703) 604-8937 (DSN 664-8937) or fax (571) 372-7469.

Suggestions for Audits

To suggest or request audits, contact the Office of the Deputy Inspector General for Auditing by phone (703) 604-9142 (DSN 664-9142), by fax (571) 372-7461, or by mail:

ODIG-AUD (ATTN: Audit Suggestions)
Department of Defense Inspector General
4800 Mark Center Drive (Room 12E25)
Alexandria, VA 22350-1500



Acronyms and Abbreviations

ASD(HD&ASA)	Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs
CAL	Critical Asset List
CIP-MAA	Critical Infrastructure Protection-Mission Assurance Assessment
DASD	Deputy Assistant Secretary of Defense for Manufacturing and Industrial Base Policy
DCI	Defense Critical Infrastructure
DCIP	Defense Critical Infrastructure Program
DCMA	Defense Contract Management Agency
DIB	Defense Industrial Base
DISLA	Defense Infrastructure Sector Lead Agent
HSPD-7	Homeland Security Presidential Directive 7
NIPP	National Infrastructure Protection Plan
PDUSD(P)	Principal Deputy Under Secretary of Defense for Policy
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(P)	Under Secretary of Defense for Policy



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

March 13, 2012

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Vulnerability and Risk Assessments Needed to Protect Defense
Industrial Base Critical Assets (Report No. DODIG-2012-064)

~~(FOUO)~~ We are providing this report for review and comment. The Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs officials did not ensure that the Defense Contract Management Agency performed vulnerability assessments in accordance with annual goals, completed risk assessments, and developed risk mitigation plans, when needed. Consequently, DoD cannot determine the level of risk to non-Government-owned assets that support critical missions and cannot forecast the likelihood of continuing operations to prevent a potential DoD mission degradation or failure. We considered management comments on a draft of this report when preparing the final report.

DoD Directive 7650.3 requires that recommendations be resolved promptly. We received comments from the Under Secretary of Defense for Acquisition, Technology, and Logistics; the Under Secretary of Defense for Policy; and the Defense Contract Management Agency on recommendations made in this report. The comments from the Under Secretary of Defense for Acquisition, Technology, and Logistics for Recommendation 1 were not responsive. Therefore, we request that the Under Secretary of Defense for Acquisition, Technology, and Logistics provide revised comments on Recommendation 1 by May 14, 2012.

If possible, send a .pdf file containing your comments to audros@dodig.mil. Copies of your comments must have the actual signature of the authorizing official for your organization. We are unable to accept the /Signed/ symbol in place of the actual signature. If you arrange to send classified comments electronically, you must send them over the SECRET Internet Protocol Router Network (SIPRNET).

We appreciate the courtesies extended to the staff. Please direct questions to me at (703) 604-8866 (DSN 664-8866).

Alice F. Carey
Assistant Inspector General
Readiness, Operations, and Support

cc:
Director, Acquisition Resources, and Analysis

~~FOR OFFICIAL USE ONLY~~

DISTRIBUTION:

DEPUTY SECRETARY OF DEFENSE
UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND
LOGISTICS
UNDER SECRETARY OF DEFENSE FOR POLICY
UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE
CHIEF, NATIONAL GUARD BUREAU
ASSISTANT SECRETARY OF DEFENSE FOR HOMELAND DEFENSE AND
AMERICAS' SECURITY AFFAIRS
ASSISTANT TO THE SECRETARY OF DEFENSE FOR NUCLEAR AND
CHEMICAL AND BIOLOGICAL DEFENSE PROGRAMS
ASSISTANT SECRETARY OF THE AIR FORCE FOR FINANCIAL MANAGEMENT
AND COMPTROLLER
DIRECTOR, DEFENSE CONTRACT MANAGEMENT AGENCY
DIRECTOR, DEFENSE LOGISTICS AGENCY
DIRECTOR, JOINT STAFF
NAVAL INSPECTOR GENERAL
AUDITOR GENERAL, DEPARTMENT OF THE ARMY
AUDITOR GENERAL, DEPARTMENT OF THE AIR FORCE



Results in Brief: Vulnerability and Risk Assessments Needed to Protect Defense Industrial Base Critical Assets

What We Did

DoD is responsible for the Defense Industrial Base (DIB) risk management. Our objective was to determine whether DoD performed DIB vulnerability and risk assessments to ensure critical assets were properly protected and to determine whether mitigation plans were in place to cover critical assets. We reviewed both national and Defense DIB requirements and assessed DoD's execution of these policies.

What We Found

~~(FOUO)~~ Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (ASD[HD&ASA]) officials did not ensure that the Defense Contract Management Agency (DCMA) performed vulnerability assessments in accordance with annual goals, completed risk assessments, and developed risk mitigation plans, when needed. From FY 2006 through FY 2010, ASD(HD&ASA) officials established a goal of ~~(FOUO)~~ vulnerability assessments on a universe of ~~(FOUO)~~ assets; however, DCMA only completed ~~(FOUO)~~ vulnerability assessments. During that same period, DCMA officials did not complete risk assessments or risk mitigation plans for critical assets. These conditions occurred because ASD(HD&ASA) officials developed policy that did not:

- address the voluntary nature of the vulnerability assessment process or
- ensure that risks for the non-Government-owned DIB assets were assessed and communicated to decisionmakers.

~~(FOUO)~~ Without complete risk assessments, DoD decisionmakers could not determine risks to DIB critical assets. Thus, DoD could not determine the level of risk to non-Government-owned assets that supported critical missions and could not forecast the likelihood of continuing operations to prevent a potential DoD mission degradation or failure. Additionally, according to cost data obtained

from the National Guard Bureau, DoD spent at least \$16 million on vulnerability assessments that were not used to perform Defense Critical Infrastructure Program risk assessments and did not result in mitigation plans.

What We Recommend

~~(FOUO)~~ We recommend that the Under Secretary of Defense for Acquisition, Technology, and Logistics amend acquisition policy to ensure DoD can obtain vulnerability information from contractors in a timely manner.

~~(FOUO)~~ We recommend that the Under Secretary of Defense for Policy, request that DoD Directive 3020.40, "DoD Policy and Responsibilities for Critical Infrastructure," January 14, 2010, (or most current edition) be amended to exclude the DIB, and create new DIB-specific criteria that define risk management requirements, roles and responsibilities for non-Government owned critical assets.

~~(FOUO)~~ We recommend that the Director, DCMA, conduct a review to ensure risk assessments are performed on all DIB facilities that have vulnerability assessments, and include in policy that vulnerability assessments are scheduled only after threat and hazard information is available.

Management Comments and Our Response

Comments from the Under Secretary of Defense for Policy were fully responsive. Comments from DCMA were fully responsive. Comments from the Under Secretary of Defense for Acquisition, Technology, and Logistics were not responsive. For a complete text of management comments, please see pages 20 through 34. We request that management provide comments on the final report by May 14, 2012. Please see the recommendations table on page ii.

Recommendations Table

Management	Recommendations Requiring Comment	No Additional Comments Required
Under Secretary of Defense for Acquisition, Technology, and Logistics	1	
Under Secretary of Defense for Policy		2.a and 2.b
Director, Defense Contract Management Agency		3.a and 3.b

Please provide comments by May 14, 2012.

Table of Contents

Introduction	1
Objective	1
Background	1
Review of Internal Controls	4
Finding. Defense Industrial Base Risk Management Process Requirements Not Met	5
Criteria for the Defense Critical Infrastructure Program	5
Insufficient Oversight of the Risk Management Process	6
Policy for Vulnerability Assessments Did Not Address the Voluntary Nature of the Process	7
Policy for Risk Management Did Not Ensure Risks Were Assessed or Communicated	8
Review of Operational Oversight Needed	9
Conclusion	10
Management Comments on the Finding and Background and Our Response	11
Recommendations, Management Comments, and Our Response	13
Appendices	
A. Scope and Methodology	16
Use of Computer-Processed Data	17
Prior Coverage	17
B. Defense Industrial Base Key Stakeholders	19
Management Comments	
Under Secretary of Defense for Acquisition, Technology, and Logistics	20
Under Secretary of Defense for Policy	22
Defense Contract Management Agency	34

Introduction

Objective

Our objective was to determine whether DoD performed Defense Industrial Base (DIB) vulnerability and risk assessments to ensure critical assets were properly protected and to determine whether mitigation plans were in place to cover critical assets. See Appendix A for a discussion of the scope and methodology and prior coverage related to the objective.

Background

DoD defines its DIB as the DoD, government, and private sector worldwide industrial complex with capabilities to research, develop, design, produce, and maintain military weapon systems, subsystems, components, or parts to meet military requirements. The DIB includes hundreds of thousands of domestic and foreign entities and their subcontractors performing work for DoD and other Federal agencies. The DIB provides Defense-related products and services that equip, inform, mobilize, deploy, and sustain forces conducting military operations worldwide. The President, DoD, and the Department of Homeland Security also recognized the DIB as a part of the Nation's critical infrastructure. See Appendix B for a chart depicting the DIB key stakeholders and the hierarchy of operational responsibilities.

National Policy

Homeland Security Presidential Directive 7 (HSPD-7), "Critical Infrastructure Identification, Prioritization, and Protection," December 17, 2003, establishes, "a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks." HSPD-7 assigns DoD as the DIB Sector-Specific Agency responsible for implementing the national-level critical infrastructure requirements and its own internal critical infrastructure protection. DoD designated the Under Secretary of Defense for Policy (USD[P]) as the office of primary responsibility for both the national and Defense-level critical infrastructure protection roles. The USD(P) further delegated those responsibilities to the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (ASD[HD&ASA]).

In June 2006, the Department of Homeland Security published the National Infrastructure Protection Plan (NIPP). The NIPP implements HSPD-7 and provides a comprehensive risk management framework for integrating the Nation's critical infrastructure initiatives into a single national effort. The NIPP implements the national protection requirement through 18 sectors.¹ The sectors include Agriculture and Food, DIB, Water, Communications, Energy, and other critical areas.

¹ A sector is a logical collection of assets, systems, or networks that provide a common function to the economy, Government, or society.

Defense Policy

DoD policy includes its national and DoD-wide protection responsibilities under the Defense Critical Infrastructure Program (DCIP). According to DoD policy, the DCIP is a risk management program that seeks to ensure availability of Defense Critical Infrastructure (DCI). A series of policies govern the DCIP, including directives, an instruction, and manuals. Key DCIP policies include:

- DoD Directive 3020.40, “DoD Policy and Responsibilities for Critical Infrastructure,” January 14, 2010, establishes the DCIP and responsibilities for program management and program support elements, including Defense Infrastructure Sector Lead Agent (DISLA), intelligence collection, and National Guard support; and
- DoD Instruction 3020.45, “Defense Critical Infrastructure Program Management,” April 21, 2008, creates policy that supports DCIP requirements and delegates oversight of DCIP implementation to the ASD(HD&ASA). This Instruction requires asset owners to determine risks to their critical assets based on information provided through program support.

Program supporting elements, such as the Under Secretary of Defense for Intelligence, implement their DCIP responsibilities through internal policy.

~~(FOUO)~~ DoD’s agency-wide DCIP identified 10 sectors critical to DoD operations and missions. Each sector has a designated DISLA. The Defense Contract Management Agency (DCMA) is the DISLA for the DIB and is responsible for implementing and executing DIB DCIP requirements. In 2009, the DIB contained about 300,000 assets. From that universe, DCMA personnel identified the most critical assets and prioritized them on the Critical Asset List (CAL), and then used the CAL to identify assets for DIB vulnerability assessments. The ASD(HD&ASA) set goals for the number of assessments to be performed each year.

National Guard’s Process for Critical Infrastructure Protection – Mission Assurance Assessments

~~(FOUO)~~ According to the 2008 DCIP Strategy, DoD uses the National Guard’s existing Critical Infrastructure Protection – Mission Assurance Assessments (CIP-MAA) process to execute DIB vulnerability assessments. The DCIP strategy explains that the National Guard’s existing mission to protect critical infrastructure supporting both the Federal Government and State governors provided “an ability to serve as a liaison between DCIP and local commercial infrastructure providers and members of the DIB regarding National Guard matters.” In this regard, the National Guard may facilitate DIB asset vulnerability assessments.

Risk Management Process Overview

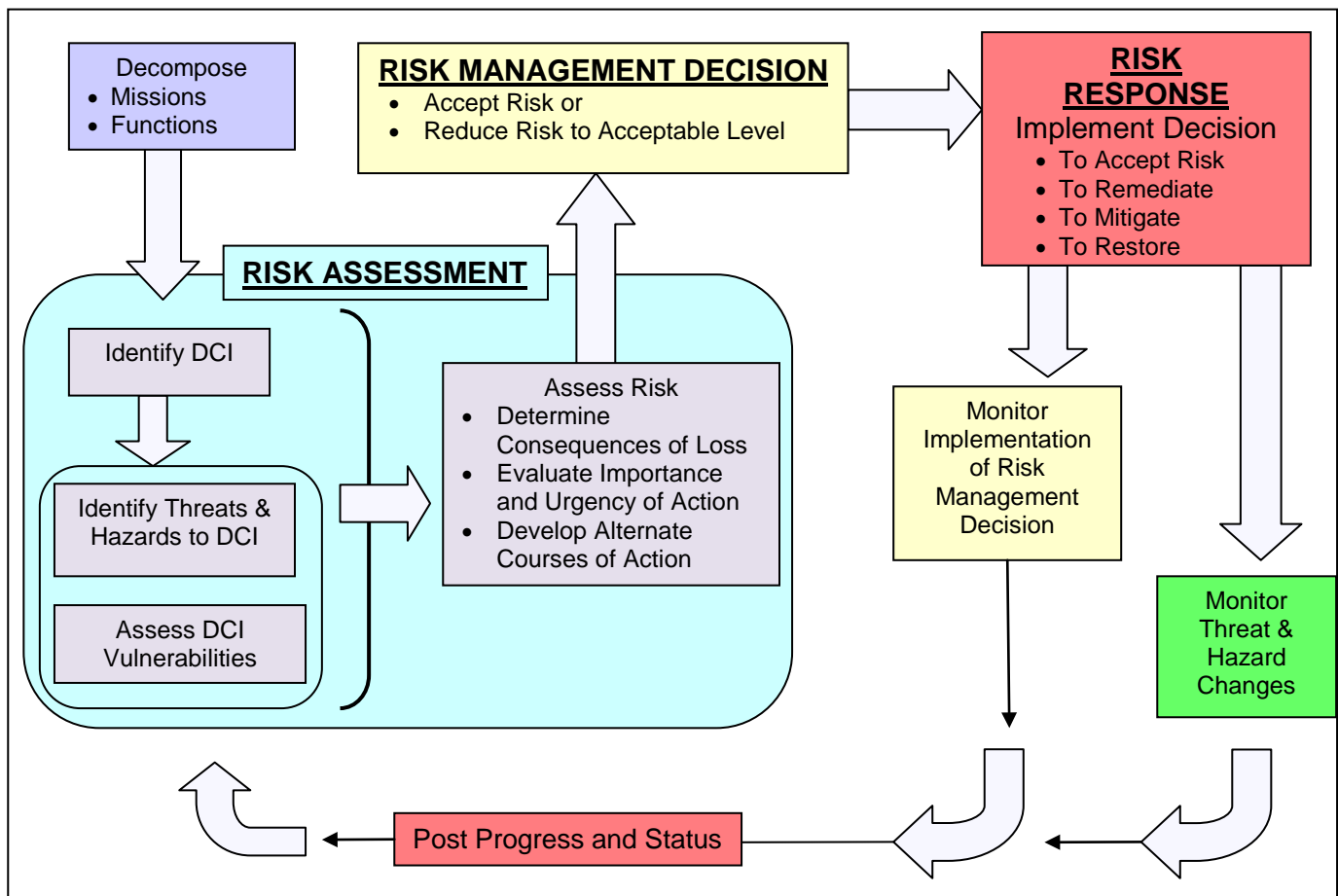
Risk management is a process by which decisionmakers accept, reduce, or offset risk and subsequently make decisions that weigh overall risk against mission benefits.

The following are the components of the DCIP risk management process:

- Risk Assessment
 - Identify and prioritize critical infrastructure
 - Obtain threat assessments and hazard information
 - Conduct vulnerability assessments
- Risk Management Decision
 - Accept risk (no risk response)
 - Respond to risk
- Risk Response
 - Remediation
 - Mitigation
 - Reconstitution

Our audit focused on the risk management process. The risk management process includes vulnerability assessments, risk assessments, and mitigation plans. Mitigation plans are the result of the risk response decision to mitigate the risk. The following figure depicts the DoD Risk Management Process Model.

Figure. Risk Management Process Model



Source: DoD Instruction 3020.45, "Defense Critical Infrastructure Program Management," April 21, 2008.

~~(FOUO)~~ DCIP policy identifies many participants in the risk management process; two of which are a mission owner and an asset owner. For the DIB, the mission owner is the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD[AT&L]) because USD(AT&L) owns the mission to acquire weapons systems and has the support required to maintain the systems. In this scenario, an asset owner would be an entity that owns the facility that produces, maintains, or repairs the weapons systems needed for such missions. According to DCMA officials, about 94.5 percent of DIB critical assets are non-Government-owned. DCMA is responsible for coordinating with the non-Government asset owner to complete risk management activities. DoD Instruction 3020.45 states that the DIB DISLA, as the asset owner's representative, is responsible for:

- submitting a prioritized assessment list,
- requiring the use of threat and hazard information in assessments,
- conducting vulnerability assessments, and
- providing risk response priorities to decisionmakers.

Although the Instruction directs DCMA to obtain or conduct all the components of a risk assessment, it does not explicitly direct DCMA to execute the risk assessment. The Instruction directs the asset owner to conduct the risk assessment. However, DoD has no authority to direct a non-Government-owned critical asset owner to conduct a risk assessment.

Review of Internal Controls

DoD Instruction 5010.40, "Managers' Internal Control Program (MICP) Procedures," July 29, 2010, requires DoD organizations to implement a comprehensive system of internal controls that provides reasonable assurance that programs are operating as intended and to evaluate the effectiveness of the controls. We determined internal control weaknesses existed within the risk management process. Specifically, for the DIB sector, ASD(HD&ASA) officials did not:

- maintain oversight of the risk management process; and
- establish clear guidance for the DIB critical asset risk management process.

We will provide a copy of the report to the senior official responsible for internal controls in the Office of the USD(P).

Finding. Defense Industrial Base Risk Management Process Requirements Not Met

~~(FOUO)~~ ASD(HD&ASA) officials did not ensure that DCMA performed vulnerability assessments in accordance with annual goals, completed risk assessments, and developed risk mitigation plans, when needed. From FY 2006 through FY 2010, ASD(HD&ASA) officials established a goal of ~~(b) (3)~~ vulnerability assessments on a universe of ~~(b) (3)~~ assets; however, DCMA officials only completed ~~(b) (3)~~ vulnerability assessments. During that same period, DCMA officials did not complete risk assessments or risk mitigation plans for DIB critical assets. These conditions occurred because ASD(HD&ASA) officials developed policy that did not:

- address the voluntary nature of the vulnerability assessment process or
- ensure that risks for the non-Government-owned DIB assets were assessed and communicated to decisionmakers.

~~(FOUO)~~ Without complete risk assessments, DoD decisionmakers could not determine risks to DIB critical assets. Consequently, DoD could not determine the level of risk to non-Government-owned assets that supported critical missions and could not forecast the likelihood of continuing operations to prevent a potential DoD mission degradation or failure. Additionally, according to cost data obtained from the National Guard Bureau, DoD spent at least \$16 million on vulnerability assessments that were not used to perform DCIP risk assessments and did not result in mitigation plans.

Criteria for the DCIP

DoD Instruction 3020.45, states that the ASD(HD&ASA), under the direction and control of the USD(P), is required to provide:

- policy and guidance for the DCIP and oversee the implementation of:
 - DISLA responsibilities,
 - DCI vulnerability assessments conducted in accordance with established DCIP standards and benchmarks, and
 - risk assessments;
- recommended changes to USD(AT&L) for the Federal Acquisition Regulation, the Defense Federal Acquisition Regulation Supplement, and other procurement regulations as appropriate to implement DCIP; and
- requirements to the Under Secretary of Defense for Intelligence for intelligence collection, threat assessments, and dissemination of warnings regarding DCI.

The DIB is one of the 10 sectors of the DCIP and DoD did not develop separate DIB-specific policy, or language in DCIP policy that excludes the DIB. Therefore, DCIP policy applies to the DIB.

² The CAL had three versions within the scope of our audit. We compared the three versions and identified ~~(b) (3)~~ unique assets identified from FY 2006 through FY 2010.

Criteria for Critical Assets

~~(FOUO)~~ DCMA personnel used the annual DIB CAL to prioritize DIB critical assets and to schedule them for assessments. According to DCIP policy, a critical asset is “a specific entity that is of such extraordinary importance that its incapacitation or destruction would have a very serious, debilitating effect on the ability of a nation to continue to function effectively.” ~~(FOUO)~~ OSD/JS: (b) (3), 10 USC § 130e

~~(FOUO)~~

- ~~(FOUO)~~ OSD/JS: (b) (3), 10 USC § 130e
- ~~(FOUO)~~
- ~~(FOUO)~~
- ~~(FOUO)~~

~~(FOUO)~~

OSD/JS: (b) (3), 10 USC § 130e

Insufficient Oversight of the Risk Management Process

Although ASD(HD&ASA) officials were responsible for oversight of the risk management process, they did not ensure that DCMA officials met annual vulnerability assessment goals. Additionally, DCMA officials did not complete risk assessments or mitigation plans.

Vulnerability Assessments Not Performed in Accordance With Annual Goals

~~(FOUO)~~ The Defense Infrastructure Sector Assurance Plans, published by DCMA, include ASD(HD&ASA)-established annual goals for the number of vulnerability assessments. ASD(HD&ASA) officials established the first goal of ~~(FOUO)~~ vulnerability assessments in 2007, following the 2006 pilot year for which goals were not yet established. The table on page 7 shows the goals, the number of vulnerability assessments performed per year, the number of DIB critical assets identified, and the percentage of the annual goals met each year. ASD(HD&ASA) officials explained that they set vulnerability assessment goals rather than established a requirement for a minimum number of assessments because non-Government-owned asset participation was not mandatory. They further explained that the difficulty in obtaining access to non-Government-owned facilities became evident as DCMA officials attempted to perform the first assessments in FYs 2006 and 2007. During that period, when DCMA officials contacted critical asset owners to request access, the asset owners often denied the request.

~~(FOUO)~~ **Table. DCMA Vulnerability Assessments Performed Versus Assessment Goals**

Calendar Year	Assessment Goal	Assessments Performed	Number of Critical Assets	Percentage of Goal
2006	N/A ¹	OSD/JS: (b) (3), 10 USC § 130e	OSD/JS: (b) (3), 10 USC § 130e	N/A
2007	OSD/JS: (b) (3), 10 USC § 130e			percent
2008				percent
2009				percent
2010				percent
Total				percent

¹ 2006 was the pilot year for CIP-MAAs and did not have a specified goal.

² This represents the number of unique assets between the three lists. See note on page 5.

Risk Assessments and Mitigation Plans Not Completed

~~(FOUO)~~ ASD(HD&ASA) officials did not ensure risk assessments were completed and risk mitigation plans were developed, when needed. According to DCMA officials, about 94.5 percent of the DIB critical assets were non-Government-owned. Because DCIP policy assigned the risk assessment responsibility to the asset owner and ASD(HD&ASA) personnel took the position that DoD could not enforce the risk assessment requirement on a non-Government asset owner, ASD(HD&ASA) officials did not ensure risk assessments were completed. Without risk assessments, management could not determine whether the most appropriate risk response for a critical asset was to mitigate the risk and develop a mitigation plan.

Policy for Vulnerability Assessments Did Not Address the Voluntary Nature of the Process

~~(FOUO)~~ Although the difficulty in obtaining access to non-Government-owned facilities became evident as DCMA officials attempted to perform the first vulnerability assessments, ASD(HD&ASA) did not address the voluntary nature of the assessment process in policy. Additionally, ASD(HD&ASA) did not ensure acquisition policy changes were made to address this issue.

Voluntary Approach Did Not Ensure Access to the Most Critical Assets

~~(FOUO)~~ DCMA officials did not meet program goals for the number of vulnerability assessments conducted because contractors were subject to these assessments on a voluntary basis. According to DCMA officials, obtaining contractor approval before conducting an assessment hindered performing a vulnerability assessment. They discussed the lengthy process used to obtain approval, then schedule and prepare the assessment teams to complete the assessment. One example showed that more than 4 months transpired from initial contact to the assessment because of approval and scheduling delays. From FY 2006 through FY 2010, DCMA officials did not conduct

vulnerability assessments based on the assets' ranked criticality, but instead conducted vulnerability assessments on those assets whose owners volunteered for assessments. This voluntary approach did not meet the intent to manage risks to prioritized DIB assets or ensure that DCMA officials gained access to the most critical assets.

Acquisition Policy Change Needed

~~(FOUO)~~ ASD(HD&ASA) personnel need to recommend a change to the DIB facility contracting process that requires contractors to provide vulnerability information to DCMA within a specific period, so DoD can manage risks to its continued operations. DoD Directive 3020.40 requires that ASD(HD&ASA) provide the USD(AT&L) with recommended changes to the Federal Acquisition Regulation, the Defense Federal Acquisition Regulation Supplement, and other procurement regulations as appropriate to implement DCIP. ASD(HD&ASA) personnel stated that they held discussions with personnel from USD(AT&L) about adding a clause to DIB contracts that required vulnerability assessments. When asked about the implications of acquisition policy changes, USD(AT&L) representatives stated they believed this would involve associating an incentive within the contracts because it would require contractors to conduct additional work. While this requirement might increase contracting costs to DoD, not having vulnerability information needed to assess and plan for risks did not meet the intent of HSPD-7. DoD could meet the intent of HSPD-7, as it relates to vulnerability assessments, by:

- continuing the use of the CIP-MAA teams,
- using vulnerability assessments performed by other government entities, and
- using self-assessments tailored for each critical asset by DCMA and completed by the asset owners.

Policy for Risk Management Did Not Ensure Risks Were Assessed or Communicated

~~(FOUO)~~ DCIP policy does not clearly define the roles and responsibilities of the risk management process. As a result, DCMA did not complete risk assessments of DIB critical assets. Additionally, DCMA did not have risk assessment information to communicate to decisionmakers.

Assessment Responsibilities Not Clearly Defined in Policy

~~(FOUO)~~ ASD(HD&ASA) personnel did not provide implementing policy related to DISLA responsibilities for DIB risk management. DoD Directive 3020.40 requires that ASD(HD&ASA) provide policy and guidance for the DCIP and oversee the implementation of DISLA responsibilities. DCMA personnel wrote a majority of the implementation policy and later obtained ASD(HD&ASA) agreement.

In essence, DCMA personnel were responsible for writing their own performance objectives.

For example, DCMA personnel wrote their statements of work according to a plan that they developed and proposed to ASD(HD&ASA). In essence, DCMA personnel were responsible for writing their own performance objectives.

~~(FOUO)~~ According to DoD Instruction 3020.45, the DISLA is responsible for performing or obtaining the three components of a risk assessment. For the DIB, this is DCMA. However, the Instruction assigns the responsibility for conducting risk assessments to “asset owners.” As previously stated, ASD(HD&ASA) personnel have taken the position that DoD could not enforce the risk assessment requirement on a non-Government asset owner. Ignoring the risk assessment requirement because an asset is non-Government-owned did not meet the intent of the DCIP and did not allow DoD risk managers to manage risks to the DIB critical assets upon which its mission depends.

~~(FOUO)~~ DCMA, as the asset owner’s representative, could have done risk assessments on the ^{OS}~~(S)~~ assets for which it had vulnerability information, but they did not have required threat assessments for most of the period audited. DCMA personnel received threat information from a designated field activity, but they only received counterintelligence information and not a threat assessment required by the DCIP risk management process. DCMA personnel explained that they used counterintelligence information provided by a

Without threat information, responsible parties cannot complete risk assessments or develop plans to mitigate risks.

designated field activity until about 2008, when the field activity was reorganized. They also stated that they obtained counterintelligence information from a U.S. Army Military Intelligence unit; however, the information was sporadic. Threat assessment products are not just

counterintelligence, but include all related intelligence from DoD and other Federal and State law enforcement entities. Without threat information, responsible parties cannot complete risk assessments or develop plans to mitigate risks.

~~(FOUO)~~ Based on cost data obtained from the National Guard Bureau, DoD spent at least \$16 million since FY 2006 to conduct voluntary vulnerability assessments that did not result in corresponding risk assessments. DCMA officials should:

- perform risk assessments on all DIB facilities that have vulnerability assessments, and
- schedule vulnerability assessments only after ensuring the availability of threat assessments.

Risk Information Not Communicated

~~(FOUO)~~ Because DCMA did not complete risk assessments, they did not have information to communicate to decisionmakers. According to DoD Instruction 3020.45, the DISLA is responsible for communicating the risk assessment results for non-Government-owned assets to the decisionmaker. Without risk information, decisionmakers could not make informed decisions, including whether or not mitigation plans were needed.

Review of Operational Oversight Needed

~~(FOUO)~~ ASD(HD&ASA) personnel stated that, as a policy organization, they were focusing on providing policy and were moving away from the operational functions related to the DIB. This was inconsistent with their prescribed responsibilities to

supervise DCIP functions. Additionally, the Defense Science Board's Task Force on Critical Homeland Infrastructure Protection issued a report in 2007 that identified the need for DoD to enhance its assessment programs to produce "full risk assessments." Specifically, the Task Force reported that DoD

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...each of which generates its own assessments, focuses on compliance rather than performance, and deals with current threats.

~~(FOUO)~~ The Task Force determined that DoD resources were not "matched to risk." They recommended that the Deputy Secretary of Defense designate a lead agency or office for an integrated risk management program with responsibilities to:

- consolidate the many vulnerability assessment programs into one risk assessments program that includes performance based criteria and considers the spectrum of current and future threats, and
- help identify prudent risk mitigation measures and assess progress in achieving improved levels of security.

~~(FOUO)~~ In contrast to the policy focus of ASD(HD&ASA), the USD(AT&L) Manufacturing and Industrial Base Policy has an operational focus with regard to the DIB. Specifically, their mission is to monitor, preserve, and enhance the national security industrial base of the United States. Additionally, USD(AT&L) Manufacturing and Industrial Base Policy personnel created the initial criteria that identified DIB critical assets and had detailed knowledge of the DIB sector. These personnel were familiar with the creation of the DIB CAL and the risk management process and had a working relationship with DCMA.

~~(FOUO)~~ ASD(HD&ASA) personnel should establish specific policy that clearly identifies how best to carry out the roles and responsibilities of the DCIP risk management process for the DIB. Once ASD(HD&ASA) personnel establish a new policy, they should coordinate with USD(AT&L) personnel to determine which organization is best equipped to provide operational oversight to the DIB DISLA and the DIB risk management process.

Conclusion

~~(FOUO)~~ The President of the United States and the Deputy Secretary of Defense signed national and Defense-level policy, respectively, which designated the DIB as a critical infrastructure sector. Further, both policies directed risk management and vulnerability assessments. The rationale for the existence of the national and Defense programs was to identify, prioritize, and protect critical infrastructure. DoD was responsible for doing this for the DIB at the national level and within the DoD's internal DCIP. The very nature of the DIB illustrated that its critical assets are essential to national security and the DoD missions. The DCIP Risk Management Process, if conducted, will satisfy the intent of HSPD-7 and the DCIP.

~~(FOUO)~~ ASD(HD&ASA) personnel stated that they could not conduct the DCIP Risk Management Process on the DIB because contractors own the majority of the assets. Specifically, ASD(HD&ASA) personnel did not ensure the DISLA met vulnerability assessment goals or performed risk assessments. According to cost data obtained from the National Guard Bureau, DoD spent at least \$16 million on vulnerability assessments that were not used to perform DCIP risk assessments and did not result in informed risk response decisions. Rather than abandon the risk management process, DoD should obtain vulnerability, threat, and hazard information to make informed decisions. If ASD(HD&ASA) personnel continue in their attempt to satisfy risk management requirements by allowing non-Government critical asset owners to manage their own risks, they may hinder DoD's ability to respond to a threat or hazard. If the cost of mitigation is too high, DoD may decide to assume the risk, but the DIB program execution does not provide the information needed to make these crucial decisions.

Management Comments on the Finding and Background and Our Response

Overall, the Principal Deputy Under Secretary of Defense for Policy (PDUSD[P]) disagreed with our background and finding stating that the report's broad conclusions did not take into consideration a recently coordinated strategy and proposed changes to policy that are currently in coordination. The PDUSD(P) provided detailed information on how they envision their new strategy will work. Additional points made by PDUSD(P) included:

- OASD(HD&ASA) personnel's detailed liaison work and information sharing helped to mitigate one system's "serious casualty to its manufacturing operations,"
- CIP-MAA process results were used by asset owners to make positive changes to mitigate risk,
- ASD(HD&ASA) personnel have provided more than sufficient oversight of the DIB risk management program, and
- information in the table on page 7 is accurate, but could be misleading.

Please see the Management Comment Section for PDUSD(P)'s full response to our finding and background. PDUSD(P) included four addenda to their comments on our draft report. The addenda are For Official Use Only. These addenda include:

- "Response to Draft Report 'Vulnerability Assessments Needed to Protect Defense Industrial Base Assets,' " February 3, 2012;
- "Department of Defense Mission Assurance Strategy," January 4, 2012;
- DoD Directive 3020.40, "DoD Policy and Responsibilities for Critical Infrastructure," January 14, 2010, Incorporating Change 2, XXX XX, 2012³; and
- DoD Instruction 3020, "Implementation of DoD Responsibilities as Sector Specific Agency for the Defense Industrial Base," Draft – November 18, 2011.

³ The DoD Directive provided as an addendum is pre-decisional and in draft format. The "XXX XXX" represents a placeholder on the document for when the Directive becomes final.

We are including the first addendum, which include comments on the finding and background, with PDUSD(P)'s comments on our recommendations. Addenda 2 through 4 are pre-decisional policies and not directly pertinent to the report. We will provide them upon request.

Our Response

The new approach to DCIP risk management, as described in the comments from PDUSD(P), appear comprehensive and achievable, but significantly changes the approach defined in the existing policy. During the course of the audit, we requested to review this new policy, but ASD(HD&ASA) officials stated that the policy was pre-decisional and did not release the policy to us. Further, the 2010 versions of the DoD Directive 3020.40 and the DIB Sector Specific Plan did not foreshadow such a comprehensive change in approach to DIB risk management. Therefore, we used criteria that were in effect from FY 2006 through FY 2010, which was the scope of our audit.

~~(FOUO)~~ The primary purpose of the DCIP is to protect critical infrastructure through a risk management process that produces information that enables risk decisions by DoD officials. The process includes the requirement to identify, prioritize, and conduct risk assessments on critical assets. However, the DIB DISLA performed no risk assessments on DIB critical assets during the scope of our audit. New DCIP policy cannot change the fact that DoD did not satisfy its requirement to conduct risk assessments for the 5 years reviewed.

~~(FOUO)~~ The PUSD(P) also provided an example of how a serious casualty to a facility's manufacturing operations was mitigated by OASD(HD&ASA) personnel. This example shows only what happens if a facility is "not immediately essential," but provides no scenario of what the effect could have been if the capability were immediately essential. Using this example to show how the current system works and how the proposed system will work better, ignores the fact that the assets on the CAL represent the most critical ^{OSD} percent of all DIB assets. Without a detailed review of the most critical of these assets, the impact of a slow down or stoppage of manufacturing operations cannot be assessed or mitigated in advance.

~~(FOUO)~~ Furthermore, we based our report's discussion on the CIP-MAA teams in the context of the primary requirement that the DISLA complete risk assessments using the vulnerability assessments performed by the CIP-MAA teams. We did not imply that the CIP-MAA teams were not assets or that they did not add value to the program. In fact, we asked for documentation supporting the benefits of the CIP-MAA process to contractors, but DCMA officials stated that they had none. Even without documented evidence of these benefits, we recognized the positive impact the CIP-MAAs could have and suggested that the CIP-MAA teams continue to provide the service to these DIB assets. However, we determined that those successes do not offset the lost opportunity to perform at least ^{OSD} risk assessments on critical assets for which vulnerability assessments had been completed.

Our conclusions regarding lack of oversight came from ASD(HD&ASA) and Industrial Analysis Center's responses to questions, interviews, and documentation gathered during fieldwork and from responsibilities written in the related policy. All evidence fully supported our conclusion that ASD(HD&ASA) did not perform its oversight responsibilities. In regards to the information presented in the table on page 7 of the draft report, USD(P) officials did not dispute the information presented in the table on page 7, but rather stated that the information was misinterpreted. Our audit results support our interpretation of the data.

~~(FOUO)~~ During our audit, we considered the fact that satisfying DIB risk management requirements depended mostly on the cooperation of privately held assets; however, as stated previously, proposed changes to the policy do not negate the fact that DoD wrote a requirement to conduct the risk assessments and did not satisfy that requirement for the 5 years reviewed.

Recommendations, Management Comments, and Our Response

1. ~~(FOUO)~~ We recommend that the Under Secretary of Defense for Acquisition, Technology, and Logistics amend acquisition policy to ensure DoD can obtain vulnerability information from contractors in a timely manner.

Under Secretary of Defense for Acquisition, Technology, and Logistics Comments

The Deputy Assistant Secretary of Defense for Manufacturing and Industrial Base Policy (DASD), responding for the USD (AT&L), disagreed with the recommendation. The DASD stated that implementing the recommendation would require changing the voluntary nature of the program. The DASD also stated that costs would increase significantly because of a major alteration of current DoD contracts and that contractors would pass increased costs on to the Government. Additionally, the DASD stated that USD(AT&L) intends to move away from an asset-specific risk assessment process for privately-owned infrastructure in favor of a mission-based approach. The DASD stated that under this new approach, asset-specific mitigation measures would be rare and they have already eliminated funding to support assessments of private sector assets.

Our Response

Comments from the DASD were not responsive. Although the DASD stated that there would be an increase in costs to change contracts, they provided no evidence supporting the assumption that a significant increase in contract cost would occur. On the contrary, the DIB Sector-Specific Plan, Chapter 3.1, May 2007, as input to the NIPP, recognizes that, "[l]arger companies often include some level of risk assessment as part of prudent business practices." Given that some companies are already capturing risk management data, implementing this recommendation should not incur significant costs to DoD. Under this scenario, DoD could publish a self-assessment for all contractors to fill out to ensure receipt of the data needed to assess risk on those facilities that DoD deemed most critical. Additionally, during our audit and in their response to our discussion draft, the

DASD did not discuss a mission-focused risk assessment process. We request that the USD(AT&L) provide evidence to support the significant increase in contract costs and additional comments in response to the final report that identify how the new mission-focused approach will meet the intent of HSPD-7 and the NIPP.

~~(FOUO)~~ We did not analyze the affect of performing risk assessments on a broader level, but considering that each critical asset facility has different vulnerabilities, we do not see how DoD can conduct risk assessments or respond to risk if DoD does not know the facility-specific vulnerabilities. Please see the figure on page 3 for the components of the risk management process. DoD performed no risk assessments on privately-owned critical assets; therefore, DoD cannot state whether mitigation measures would be rare until the DCMA performs risk assessments.

2. ~~(FOUO)~~ We recommend that the Under Secretary of Defense for Policy:

a. Request that the Deputy Secretary of Defense, amend DoD Directive 3020.40, “DoD Policy and Responsibilities for Critical Infrastructure,” January 14, 2010, (or most current edition) to specifically exclude the Defense Industrial Base Sector.

b. Create a DoD instruction for the Defense Industrial Base Sector that sets requirements for risk management of the non-Government-owned critical assets and assigns appropriate roles and responsibilities to Under Secretary of Defense for Acquisition, Technology, and Logistics personnel.

Under Secretary of Defense for Policy Comments

The PDUSD(P), responding for the Under Secretary of Defense for Policy, partially agreed with the recommendations. Specifically, the PDUSD(P), stated that DoD Directive 3020.40, as currently written, does not provide sufficient guidance for private-owned DIB assets. However, the ASD(HD&ASA) coordinated a DoD Mission Assurance Strategy that provides an overarching framework for risk management for all defense critical infrastructure. The PDUSD(P), further stated that although they would not exclude the DIB Sector from DoD Directive 3020.40 as recommended, they would amend the Directive to reflect the new strategic framework and clarify the incorporation of non-DoD owned defense critical infrastructure. Additionally, the PDUSD(P) agreed with our recommendation to create a DoD instruction for the DIB sector that sets risk management requirements for non-Government owned critical assets and assigns appropriate roles to the USD(AT&L). Lastly, the PDUSD(P) provided examples of the DIB risk management initiatives underway for specific DIB assets.

Our Response

The comments of the PDUSD(P) were responsive, and no further comments are required.

3. ~~(FOUO)~~ We recommend that the Director, Defense Contract Management Agency:

a. Conduct a review to ensure the Defense Contract Management Agency Industrial Analysis Center performs risk assessments on all DIB facilities that have vulnerability assessments.

b. Include in policy that vulnerability assessments should not be conducted on critical assets until threat and hazard information is available to complete a risk assessment.

DCMA Comments

The Executive Director, Portfolio Management & Integration, DCMA, agreed with the recommendations. The Executive Director stated that DCMA would obtain risk assessments before performing vulnerability assessments in the future. Additionally, the Executive Director, Portfolio Management & Integration, agreed with developing internal procedures for threat and hazard assessments before performing future assessments.

Our Response

The comments of the Executive Director, Portfolio Management & Integration, were responsive. No further comments are required.

Appendix A. Scope and Methodology

We conducted this performance audit from February 2011 through October 2011 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. The evidence obtained for this audit provides a reasonable basis for our findings and conclusions based on our audit objectives.

Our objective was to determine whether DoD was performing DIB vulnerability assessments and risk assessments to ensure critical assets were properly* protected and whether mitigation plans were in place to cover critical assets. We determined that DCIP vulnerability assessments began in FY 2006, so the scope of our audit covered from FY 2006 through FY 2010. We asked ASD(HD&ASA) officials to provide us with lists of critical assets, vulnerability assessments, and risk assessments for that period.

~~(FOUO)~~ DCMA officials provided us with the list of vulnerability assessments, and information on their process for obtaining threat and hazard data. We requested and received three approved and one proposed DIB CAL from ASD(HD&ASA) officials. We also found evidence that sometimes, DCMA officials used a CAL still awaiting final signature as a working list for scheduling vulnerability assessments. We did not audit the accuracy of the CAL because the comprehensive nature of CAL development demanded a separate audit, which is on our FY 2012 audit plan. We used the number of critical assets per FY listed in the table on page 7 for our calculations.

~~(FOUO)~~ We compared vulnerability assessment documentation to requirements in DoD policy, including DoD Instruction 3020.45, "Defense Critical Infrastructure Program (DCIP) Management," April 21, 2008. We used this information to determine the number of DIB critical asset vulnerability assessments and risk assessments performed. Although the CAL may not be accurate, it did not affect the overall results and conclusion of this report.

Again, using the DoD Instruction 3020.45, we compared risk assessment requirements and policies governing mitigation plans against work performed during the audit's scope.

~~(FOUO)~~ We originally intended to take a sample of critical assets from the CALs and review the corresponding vulnerability assessments, risk assessments, and mitigation plans. Subsequently, we learned DCMA performed only ^{OS}~~(b)(7)(F)~~ vulnerability assessments. We reviewed all CIP-MAA reports and verified the ^{OS}~~(b)(7)(F)~~ assessments were performed on CAL assets. We also reviewed a CIP-MAA assessment template and a completed report to determine if the CIP-MAAs met approved DCIP standards.

~~(FOUO)~~ Further, we learned that DCMA did not perform DCIP risk assessments and did not complete mitigation plans. Therefore, no risk assessments or mitigation plans were available for review.

* The audit team defined "properly" as in accordance with DoD policy.

To obtain an understanding of the intent of the DCIP, implementation of DoD policy, and respective roles and responsibilities, we conducted site visits at the following locations:

- ASD(HD&ASA) in Arlington, Virginia;
- USD(AT&L) in Arlington, Virginia;
- DCMA Industrial Analysis Center in Philadelphia, Pennsylvania;
- Defense Intelligence Agency in Arlington, Virginia;
- National Guard Bureau in Arlington, Virginia;
- West Virginia National Guard CIP-MAA team in Charleston, West Virginia; and
- Joint Interagency Training and Education Center in Charleston, West Virginia.

We also reviewed the following criteria to identify DIB DCIP management roles and responsibilities of supporting organizations, and reporting requirements:

- HSPD-7, “Critical Infrastructure Identification, Prioritization, and Protection,” December 17, 2003;
- DoD Directive 3020.40, “DoD Policy and Responsibilities for Critical Infrastructure,” August 19, 2005, and July 1, 2010; and
- DoD Instruction 3020.45, “Defense Critical Infrastructure Program (DCIP) Management,” April 21, 2008.

~~(FOUO)~~ Based on cost data obtained from the National Guard Bureau, we estimated that vulnerability assessments performed by the National Guard CIP-MAA teams from FY 2006 through FY 2010 cost at least \$16 million. We based the estimate on CIP-MAA team members’ salaries and travel costs. Our estimate does not represent a fully burdened cost that may also include training and operational overhead at the National Guard or DMCA. We intended to use the estimate to emphasize the need for DoD to use the CIP-MAA results, rather than evaluate process efficiencies.

Use of Computer-Processed Data

We did not rely on computer-processed data in developing our findings, conclusions, or recommendations.

Prior Coverage

During the last 5 years, the Government Accountability Office (GAO) and the Department of Defense Office of Inspector General (DoD OIG), and the Navy have issued five reports discussing DCI. Unrestricted GAO reports can be accessed over the Internet at <http://www.gao.gov>. Unrestricted DoD OIG reports can be accessed at <http://www.dodig.mil/audit/reports>. Naval Audit Service reports are not available over the Internet.

GAO

GAO Report No. GAO-09-740R, “Defense Critical Infrastructure: Actions Needed to Improve the Consistency, Reliability, and Usefulness of DoD’s Tier 1 Task Critical Asset List,” July 17, 2009

GAO Report No. GAO-09-42, “Defense Critical Infrastructure: Developing Training Standards and an Awareness of Existing Expertise would Help DoD Assure the Availability of Critical Infrastructure,” October 30, 2008

GAO Report No. GAO-07-1077, “Defense Infrastructure: Management Actions Needed to Ensure Effectiveness of DoD’s Risk Management Approach for the Defense Industrial Base,” August 31, 2007

DoD OIG

DoD OIG Report No. IE-2006.002, “Evaluation of Defense Installation Vulnerability Assessments,” May 23, 2006

Navy

Naval Audit Service Report No. N2009-0006, “The United States Marine Corps Critical Infrastructure Program,” October 29, 2008

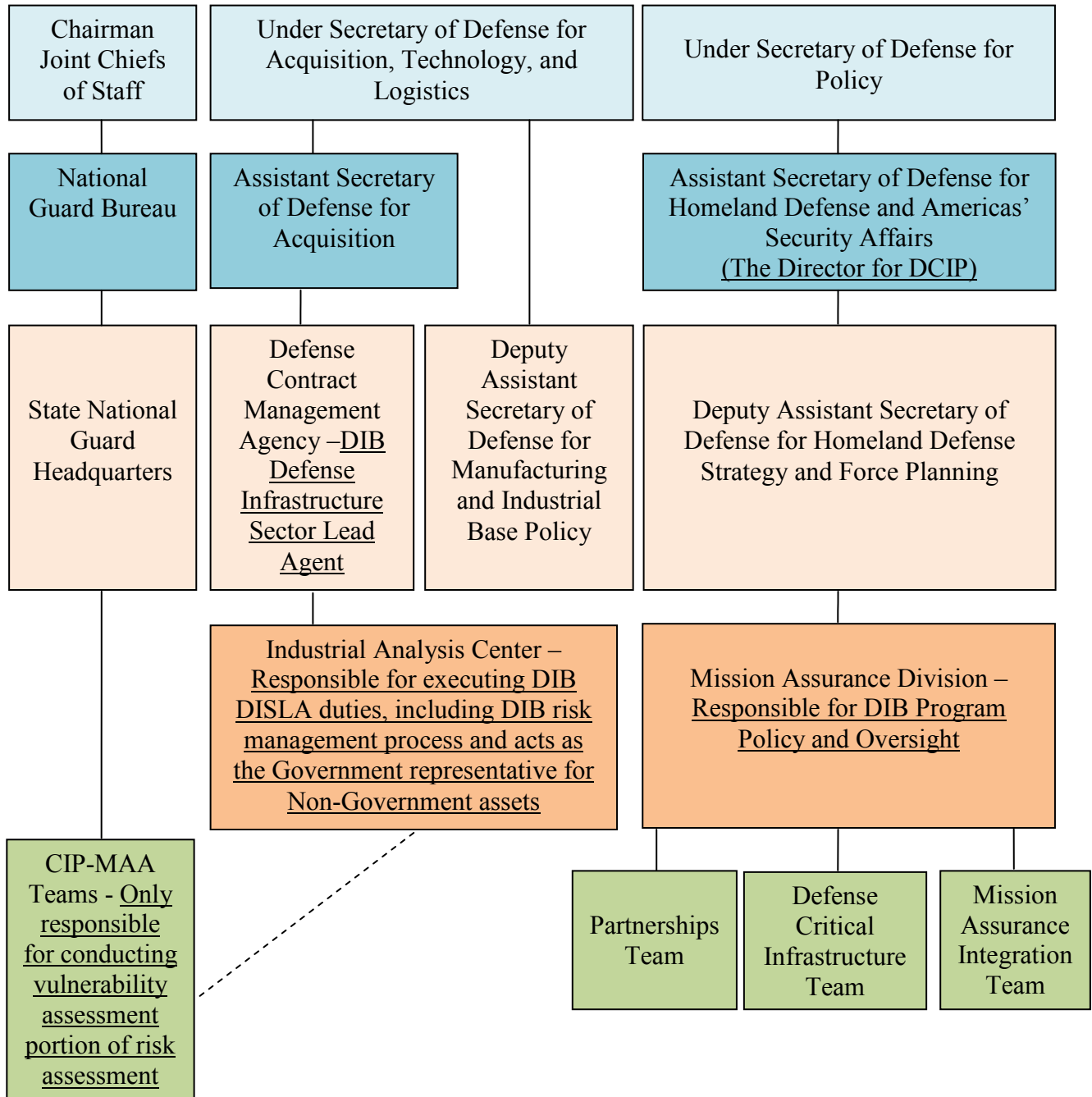
Other

“Report of the Defense Science Board Task Force on Critical Homeland Infrastructure Protection,” January 2007, under the Office of the USD(AT&L). Although not an audit service, the Defense Science Board’s Task Force on Critical Homeland Infrastructure Protection issued a report in 2007 that identified the need for DoD to enhance its assessment programs to produce “full risk assessments.”

Appendix B. DIB Key Stakeholders

The following chart illustrates the DIB operational hierarchy for key stakeholders.

Figure. DIB Operational Hierarchy



Under Secretary of Defense for Acquisition, Technology, and Logistics Comments



ACQUISITION,
TECHNOLOGY
AND LOGISTICS

OFFICE OF THE UNDER SECRETARY OF DEFENSE
3000 DEFENSE PENTAGON
WASHINGTON, DC 20301-3000

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
(Attn: Amy Matthews, Readiness, Operations, and Support)

SUBJECT: Management Response to draft report Vulnerability and Risk Assessments Needed to Protect Defense Industrial Base Critical Assets (Project No. D2011-D00LA-0100.000)

As requested, I am providing a response to the general content and recommendations contained in the subject report.

Recommendation:

We recommend that the Under Secretary of Defense for Acquisition, Technology, and Logistics amend acquisition policy to ensure DoD can obtain vulnerability information from contractors in a timely manner.

Response:

Non-Concur. The DoD IG recommended that the Under Secretary of Defense for Acquisition, Technology, and Logistics amend acquisition policy to ensure DoD can obtain vulnerability information from contractors in a timely manner. AT&L non-concurs with this recommendation. Both National and DoD approaches to privately-owned critical infrastructure currently rely on a voluntary participation model. Implementation of the DoD IG's recommendation would require a change to the voluntary participation model. DoD contracts would have to be altered to require contractors to permit DoD vulnerability assessment teams access to contractor facilities or require contractors to generate and report vulnerability information. Such requirements would incur significant costs which the contractors would pass on to the government. As currently envisioned, the Department intends to move away from an asset-specific risk assessment process for privately-owned infrastructure. Our current approach of performing vulnerability assessments has proven ineffective and is a poor use of our limited resources.

DoD has initiated the appropriate steps to move to a mission risk assessment process. This approach permits DoD to identify and track potential impacts to key programs and make programmatic adjustments where required, vice mitigation of risk at specific assets. While the identification and prioritization of critical assets will remain a central element of our approach, the assessment of risk and development of mitigation courses of action will be focused on DoD mission requirements and the ability to meet those requirements through various programmatic adjustments appropriate to the specific infrastructure dependency – the Department will assure the mission rather than the asset. Under the revised issuances, DoD anticipates that there will be no routine requirement to conduct vulnerability assessments and associated risk assessments relative to particular privately-owned infrastructure assets. In those rare cases where DoD conducts mission risk assessments and then identifies an unavoidable asset-specific mitigation

measure, the Department will engage with owners on a case-by-case basis. In support of this approach, DoD has already eliminated any funding to support assessments of private sector assets and refocused our resources on analysis and characterization of the Defense Industrial Base sector, in order to refine our ability to identify mission-specific dependencies.

Please contact [REDACTED] if additional information is required.



Brett B. Lambert
Deputy Assistant Secretary of Defense
(Manufacturing and Industrial Base Policy)

Under Secretary of Defense for Policy Comments



POLICY

~~FOR OFFICIAL USE ONLY~~

PRINCIPAL DEPUTY UNDER SECRETARY OF DEFENSE
2100 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-2100

FEB 3 2012

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

SUBJECT: Management Response to draft report Vulnerability and Risk Assessments Needed to Protect Defense Industrial Base Critical Assets (Project No. D2011-D000LA-0100.000)

Thank you for the opportunity to comment on your draft report "Vulnerability Assessments Needed to Protect Defense Industrial Base Critical Assets." We found much of the draft report to be helpful, since we are in the midst of proposing fundamental policy changes to help assure that DoD can execute its essential missions, including those missions that depend on contributions from Defense Industrial Base (DIB) assets. But we also believe that other key findings of the draft rest on inadequate data or analysis, and ask that you take our comments at Tab 1 into account in your final report.

We partially concur with your recommendation that the Under Secretary of Defense for Policy amend DoD Directive 3020.40 "DoD Policy and Responsibilities for Critical Infrastructure." We agree that as currently written, the Directive does not provide sufficient guidance for DIB assets, which are privately owned and therefore require risk management policies that differ from those tailored to government-owned assets. We disagree, however, with the draft report's recommendation that the Directive be revised to exclude the DIB. ASD(HD&ASA) recently completed coordination of a Department of Defense Mission Assurance Strategy that provides an overarching framework for risk management for all defense critical infrastructure, both private sector and government-owned (Tab 2). DoD Directive 3020.40 should be changed to reflect that overall strategic framework while also clarifying the incorporation of non-DoD owned defense critical infrastructure, to include the DIB. ASD(HD&ASA) has drafted a change to the Directive (Tab 3). We welcome your comments and suggested improvements.

We concur with your recommendation that the Under Secretary of Defense for Policy create a DoD instruction for the Defense Industrial Base Sector that sets requirements for risk management of the non-Government-owned critical assets and assigns appropriate roles and responsibilities to Under Secretary of Defense for Acquisition, Technology and Logistics. ASD(HD&ASA) has already drafted such an instruction and initiated action officer level coordination. Again, we would welcome your comments on that draft (Tab 4).

While we concur with your analysis that significant risk management challenges flow from the fact that DIB assets are privately owned, including the problems posed by the voluntary nature of some key management mechanisms, we support the Under Secretary for Defense for Acquisition, Technology and Logistics' (USD AT&L) non-concurrence with your

~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~

recommendation for obtaining vulnerability information from DoD contractors (Tab 5). USD (AT&L) found that the recommended approach would require costly changes to the existing voluntary model. Moreover, USD (AT&L) notes that DoD already intends to move away from its previous, asset-specific risk assessment process for privately owned infrastructure, which has proven ineffective and is a poor use of our limited resources.

This movement away from past policies brings me to my principal concern with the draft report and why I believe its analysis requires updating. Owing to the flaws in the pre-2010 system for risk management in both government and non-government defense critical infrastructure, ASD(HD&ASA) led a DoD-wide effort to build a more effective strategy to help assure that DoD can execute its core missions, against all hazards to defense critical infrastructure regardless of ownership. In FY2011 we ceased funding the failed approach to DIB risk management and concentrated on building (and beginning to execute on a pilot basis) a more cost-effective approach. Hence, while the report characterizes the sharp drop-off in old-style DIB vulnerability assessments as evidence of programmatic failure by ASD(HD&ASA), that drop off actually represents progress and effective management. Tab 1 suggests additional revisions to the report's findings (and the data and analysis behind them) that will more fairly capture the pivot that is already underway in DIB and non-DIB risk management.

Ongoing changes in policy also make it appropriate to revise the draft report's broadest conclusions. The Mission Assurance Strategy provides a new framework, methodological approach and management structure for risk assessment (encompassing public and private assets). Our response to the draft highlights some of our preparations to implement the Strategy and apply it to meet the specialized challenges of critical private sector assets, including the commercial power grid. These efforts are very much works in progress, however. We would welcome your rigorous critique of those efforts and your suggested improvements to them. But I would also ask that your final report not draw its broadest conclusions from failed policies of the past -- policies that we agree needed drastic changes that are now underway.

Let me offer one final suggestion on information handling. To provide data that support our proposed revisions, we have included examples of risk DIB management initiatives for specific DIB assets that are FOUO, and which I ask be referenced in your final report. More generally, a detailed discussion of vulnerabilities in the network of critical infrastructure and efforts to protect them are inherently sensitive, and therefore merit handling your final report as FOUO. Should you have any questions or concerns you may contact [REDACTED]



James N. Miller

Attachments:
As stated

~~FOR OFFICIAL USE ONLY~~

~~PRE-DECISIONAL~~
~~FOR OFFICIAL USE ONLY~~

ATTACHMENT: RESPONSE TO DRAFT REPORT "VULNERABILITY
ASSESSMENTS NEEDED TO PROTECT DEFENSE INDUSTRIAL BASE CRITICAL
ASSETS"

Response to Report in Brief Section

(U) Defense critical infrastructure protection is very much a work in progress, and we greatly appreciate the critiques and suggestions made in the draft report. In addition, however, we believe that the report would benefit from substantial revision in order to account for 1) data that the report overlooks; and 2) most important, the progress already underway to resolve the problems that the report identifies, as well as other opportunities to better achieve our ultimate objective in dealing with the DIB: that is, to strengthen DoD mission assurance.

~~(FOUO)~~ Our response parallels the structure of the draft report. We first propose changes to the report's section on defense policy. These changes form the core of our recommendations, since the transition from the failed asset-specific policies of the past to the new mission assurance framework constitutes the most important gap in the draft report's findings and recommendations. We then turn to the risk management process, where we identify some factual errors and clarify how the voluntary nature of the DIB partnership affects participation in the DCIP risk management process (and -- most important -- our shift from focusing on risks to particular assets to risks to mission execution). Next, we provide additional data on the National Guard program, including examples of how that program has added more value than the report indicates. We conclude with our response to the report's finding of inadequate internal controls. In particular, we provide data detailing our activities to provide oversight (over and above our development of the Mission Assurance Strategy). We also explain why the data on page 7 has been misinterpreted. Rather than indicating a lack of oversight, this information was noted by OASD(HD&ASA) at the time and was an essential contributor to the decision process to move away from the asset assessment process.

Response to Defense Policy Section

~~(FOUO)~~ Your characterization of existing published policy is accurate, but fails to account for work well under way, and which is already driving activities in OASD(HD&ASA). During the course of the audit, OASD(HD&ASA) staff provided information to the audit team indicating that internal review had identified a need to modify policy to incorporate evolving knowledge about the risk management of DoD dependency on non-DoD infrastructure within the DIB as well as across other sectors. OASD(HD&ASA) staff are in the process of informal staffing for a change to DoD Directive 3020.40 as well as a new DIB-oriented Instruction which is currently in internal draft form. Each of these issuances will provide formal promulgation of current activities, informed by experience.

~~(FOUO)~~ The single most significant policy development is OASD(HD&ASA)'s articulation and formalization of a DoD Mission Assurance Strategy. A mission assurance approach offers an effective and efficient means of fostering the continuous performance of

~~PRE-DECISIONAL~~
~~FOR OFFICIAL USE ONLY~~

~~PRE-DECISIONAL~~
~~FOR OFFICIAL USE ONLY~~

DoD's critical missions as well as providing for continuity of mission essential products and services across the DIB. Unfortunately, the Department's previous definitional and implementation framework for mission assurance fell short of the mark in many ways.

~~(FOUO)~~ Formerly, mission assurance was defined as a series of independent programs (such as antiterrorism; force protection; chemical, biological, radiological, and nuclear defense; defense critical infrastructure protection; installation emergency management and information assurance). This definitional construct fostered a piecemeal approach over time, vice one based on a more strategic assessment and management of risk across multiple, interrelated program areas. It has also led to a situation in which DoD installations and facilities are subjected to numerous independent program-based assessments as part of the annual assessment cycle instead of achieving the synergies, efficiencies, and cost effectiveness of a more holistic, linked approach.

~~(FOUO)~~ The Defense Critical Infrastructure Program (DCIP) and its application to the Department's roles and responsibilities as Sector Specific Agency (SSA) for the DIB, has made important progress in the mission analysis process and in the identification of assets vital to DoD's critical missions and DIB continuity. However, to this point, this process has largely focused on the identification of DoD owned physical assets and facilities that support DoD's critical missions, and has been limited in most part to physical assets and facilities. Considerations regarding human assets, information and information systems, and those supporting infrastructure systems (electricity, communication, transportation, pipelines, water, etc.) outside DoD ownership or control, yet critical to DoD mission performance and DIB continuity have not been as well integrated into the process.

~~(FOUO)~~ DoD requires a comprehensive, integrative approach to mission assurance that will lead to systematic assessment and management of risk, link protection and resilience related programs, facilitate performance measurement and process change over time, and, moreover, enable the prioritization of risk-related investments in a severely constrained fiscal environment. This process must also better incorporate non-DoD owned DIB assets that are vital to support DoD's critical missions.

~~(FOUO)~~ To achieve this goal, OASD (HD & ASA) has led an effort to develop a comprehensive new Department of Defense Mission Assurance Strategy which is fully coordinated and in the final stages of approval. ¹ This approach to mission assurance is also a key component of the revised Homeland Defense and Civil Support Strategy now under development. In the context of this Strategy, mission assurance is now more accurately defined as:

A process to protect or ensure the continued function and resilience of capabilities and assets - including personnel, equipment, facilities, networks, information and information

¹ The Mission Assurance Strategy is ready for Deputy Secretary of Defense signature but it has been placed in line first behind the Defense Strategic Guidance and now behind the Strategy for Homeland Defense and Civil Support.

~~PRE-DECISIONAL~~
~~FOR OFFICIAL USE ONLY~~

~~PRE-DECISIONAL~~
~~FOR OFFICIAL USE ONLY~~

systems, infrastructure, and supply chains - critical to the execution of DoD mission essential functions (MEFs) in any operating environment or condition.²

Through this process, the outputs of a variety of DoD mission analysis, asset criticality determination, and risk assessment activities will be linked to one another to provide an integrated input into the Department's Planning, Programming, Budgeting, and Execution (PPBE) and other decision support mechanisms. DoD will now shift its focus to actually remediating risks, instead of simply identifying vulnerabilities. This input will serve to inform decision making, resource prioritization and actions related to MEFs³ at various levels within the Department and across the DIB. The mission assurance process will also provide for better coordination and synchronization between existing DoD protection and resilience-focused programs, as well as between the Department, the DIB and other external partners.

~~(FOUO)~~ The new DoD mission assurance framework provides senior leaders at various levels across the Department with the process outputs, mechanisms, and tools they need to drive informed, risk-based *decisions and actions* regarding protection and resilience-related policies, plans, programs, and resource investments. At the installation level, maturation of this framework will enable asset and mission owners to more fully *understand and take action* to better manage shared risks, like those associated with DoD's dependency on commercial "life line" infrastructure—electricity, communications, fuel distribution and transportation. At a more strategic level, these capabilities will also foster awareness of risk issues - such as those related to cyber security - that cut across multiple DoD installations, components, or functional program areas, and impact its relationship with the DIB; enable identification of economy-of-scale solutions; and drive the selection and movement to action of DoD-wide protection and resilience priorities.

~~(FOUO)~~ This new DoD approach to mission assurance leverages existing protection and resilience programs to the greatest extent possible.⁴ The effectiveness of mission assurance will be measured in relation to mission performance in an all-threats, all-hazards environment. Mission assurance recognizes that simply protecting assets is not enough. Planning and risk management approaches must also account for creating resilience and redundancy when protection measures fail or face natural disasters, such as earthquakes, for which protection measures alone are inadequate. The mission assurance framework also acknowledges the lead role of other Federal Departments and Agencies, as well as DIB companies, commercial infrastructure owners and operators, and international partners, in coordinating strategies to

² The Mission Assurance definition used here supersedes the definition provided in the 2005 Homeland Defense and Civil Support Strategy and DoD Directive 3020.40. OASD (HD&ASA) is currently updating the mission assurance definition in DoDD 3020.40 to reflect the revised definition presented in this document.

³ Mission Essential Functions are the 31 DoD missions that must be performed continuously in any operating environment. MEFs link to the Presidentially mandated National Essential Functions and were validated and coordinated by the Deputy Assistant Secretary of Defense for Defense Continuity and Crisis Management.

⁴ Potential resources and programs affected include, but are not limited to: Antiterrorism (AT); Force Protection (FP); Defense Critical Infrastructure Protection (DCIP); Installation Emergency Management (IEM) (including Fire and Emergency Services, Explosive Ordnance Disposal, etc.); Continuity of Operations (COOP); Law Enforcement (LE); Chemical, Biological, Radiological, Nuclear and High-yield Explosive (CBRNE) Protection; Force Health Protection; and Information Assurance.

~~PRE-DECISIONAL~~
~~FOR OFFICIAL USE ONLY~~

~~PRE-DECISIONAL~~
~~FOR OFFICIAL USE ONLY~~

address risks to private sector supply chains and civilian government infrastructure that may impact DoD's critical missions.

~~(FOUO)~~ The new mission assurance framework offers new opportunities to address risks derived from DoD dependence on non-DoD owned infrastructure. When mission analysis identifies such risks there are two paths for addressing these risks. First, DoD will leverage the voluntary partnerships laid out in the *National Infrastructure Protection Plan* and associated Sector Specific Plans. Informed by an understanding of mission importance of various assets, DoD will encourage sharing of best practices and other asset-oriented risk management tools. The owners/operators will remain responsible for decisions regarding investment and innovation to assess and address risk factors appropriately. The Department must work to encourage those industries and service providers on whom it depends to design and use systems and processes that can withstand disruption and mitigate unsupportable impacts. Current partnerships with the diverse array of companies that comprise the DIB reflect the many positive benefits of such an approach. Because the number of potential partners is large and the partners appropriate to any particular issue vary widely, DoD will need to both prioritize and develop a long term, systematic framework for focusing such partnerships. Accordingly, the Department will:

- (1) Leverage existing external partner forums and processes such as those supporting interaction with the DIB.
- (2) Escalate time-sensitive, critical issues through ad hoc partnering arrangements in the absence of existing forums.

~~(FOUO)~~ A second path to address these risks requires DoD to make internal adjustments within areas that it has control over in order to mitigate the dependence a mission might have on particular DIB assets. This approach will reinforce the notion of redundancy of critical personnel and components, address single points of failure and supply chain deficiencies, encourage investment in capital modernization, and develop and test continuity plans in concert with other partners.

~~(FOUO)~~ The full integration of DIB and other private sector assets into the approach laid out in the Mission Assurance Strategy is still a work in progress. It is worth noting an example from several months ago as an illustration. A highly prioritized privately held DIB asset suffered a serious casualty to its manufacturing operations. The asset was unique in its ability to produce a critical component to a particular weapon system. A fully established mission assurance regime would have provided for rapid notification of operational organizations such as the Combatant Commanders who might be impacted by such a supply disruption. Lacking that fully implemented approach, however, OASD(HD&ASA) personnel conducted detailed liaison with the Industrial Analysis Center and the Joint Staff. The analysis validated that the component was essential to certain war plans but in the current contingency operations it was not immediately essential. Within the particular circumstances the analysts noted the event and tracked the reconstitution of the capability, but the appropriate decision makers in both the acquisition and operational hierarchies were informed. The new process identified and analyzed risk and informed appropriate decision makers, giving them the opportunity for intervention, which they deemed unnecessary in this case.

~~PRE-DECISIONAL~~
~~FOR OFFICIAL USE ONLY~~

~~PRE-DECISIONAL~~
~~FOR OFFICIAL USE ONLY~~

~~(FOUO)~~ Another example of how DoD is applying the Mission Assurance Strategy can be found in the matter of dependence on commercially-provided electric power, informed by lessons learned through working with the DIB Sector. A 2009 GAO Report on *“Actions Needed to Improve the Identification and Management of Electrical Power Risks and Vulnerabilities to DoD Critical Assets”* stated that DoD’s mission critical assets rely primarily on commercial electric power and are vulnerable to disruptions in electric power supplies.⁵

~~(FOUO)~~ The DoD fully recognizes the strategic importance of mitigating the risks posed to its critical missions by extended commercial power outages; extended outages of weeks to months at specific sites is of particular concern. The DoD is nearly 99% dependent on commercially provided power for its electricity needs at military installations. The DoD relies on electric power at its installations and facilities to deploy, support and sustain its forces and operations worldwide. Some DoD installations in the United States conduct current operations “reach back” in direct support of warfighting missions overseas. Many installations serve as a base of operations for Defense Support of Civil Authorities activities in Federal emergency relief and recovery efforts. Extended power disruptions at these installations could adversely affect power projection, warfighting and homeland defense mission capability.

~~(FOUO)~~ Commercial power sources are threatened by natural hazards and deliberate attacks, either physical and cyber in nature, that could have cascading impacts and result in extended power outages at DoD installations. These threats could lead to extended electric power disruptions that have the potential to challenge our nation’s defense capabilities. The DoD assesses risk to its mission critical assets. These risk assessments evaluate the reliability of supporting commercial electric power, the availability of back-up electric power supplies and single points of failure. DoD developed Risk Decision Packages to address risk associated with its mission critical assets. Risks deriving from electric power vulnerabilities are considered in this process, along with other mission and infrastructure related risks. These risks are reduced through existing DoD legal and budgetary authorities. In one case, for instance, an on-site natural gas co-generation facility was built to provide electricity in the event of a commercial power disruption. Risks that exist outside the purview of DoD-owned installations or facilities are addressed through interagency processes and in coordination with local commercial utility providers. This closely parallels our method for risk management with regard to dependence on DIB assets.

Response to Risk Management Process Overview Section

~~(FOUO)~~ As discussed in our response to the Defense Policy section of the report, we are revising our approach and associated policy guidance on risk management activities involving DoD mission dependency on privately held assets. For the vast majority of the DIB assets, privately held, we rely on the voluntary cooperation of the owners/operators under the construct of the National Infrastructure Protection Plan and our associated Defense Industrial Base Sector Specific Plan. This has been an evolving relationship, as we explained to your team over the course of this audit. In the early stages of the relationship we had believed that we could transfer

⁵ GAO Report 10-147, *“Defense Critical Infrastructure: Actions Needed to Improve the Identification and Management of Electrical Power Risks and Vulnerabilities to DoD Critical Assets,”* October 2009

~~PRE-DECISIONAL~~
~~FOR OFFICIAL USE ONLY~~

~~**PRE-DECISIONAL**~~
~~**FOR OFFICIAL USE ONLY**~~

the mission-oriented but asset-based risk management methods of the internal DCIP program to the external DIB Sector. To this end we supported the creation of the National Guard Critical Infrastructure Protection – Mission Assurance Assessments (CIP-MAA) and sought to make use of them in identifying, and supporting the mitigation of, risks associated with DIB assets. As we have learned, we are not able to apply DoD risk management practices directly to the privately held assets. As we have noted in our Sector Specific Plan, “DIB asset owners are encouraged to evaluate their risk management practices consistent with DoD risk management principles.”

~~(FOUO)~~ Contrary to your report’s assertion, the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) is NOT a mission owner. Although it may have policy oversight in this area – missions in DCIP policy fall into one of 3 categories – (Described in DoDM 3020.45 v1)

- Combatant Command assigned missions that support MEFs, Primary MEFs, and National Essential Functions,
- Title 10 responsibilities of the Military Departments to organize, train, and equip forces, and
- DISLA sector functions that crosscut the Department.

The mission owner responsibility that the IG incorrectly invests in the USD(AT&L) is actually part of the Military Departments Title 10 responsibilities and the DIB DISLA responsibilities.

~~(FOUO)~~ The DoD approach to risk management in the DIB Sector has evolved significantly since the original development of the CIP-MAA. The key Sector Specific Agency team effort of ASD(HD&ASA) and USD(AT&L) now leverages the analytic and outreach capability of the Defense Contract Management Agency to identify the mission dependencies of the major acquisition programs and identify the specific materiel providers that are essential to those programs. By analyzing the links of DIB assets to missions we initiate the process of managing risk to missions, rather than risk to assets. This puts the DoD risk management process to work directly on what DoD owns and can affect, which is the mission. Mitigation of risk posed to the mission by dependence on a particular asset becomes the target, rather than risk at the particular asset.

Response to National Guard Critical Infrastructure Protection – Mission Assurance Assessments Section

~~(FOUO)~~ Your report cites the CIP-MAA in a number of places. In some cases the report indicates that the National Guard teams spent \$16 million dollars to no useful end, thanks to a lack of ASD(HD&ASA) oversight. These indications are misleading. We acknowledge that CIP-MAA teams were employed without any guarantee that information would be broadly shared within DoD. Nonetheless, the CIP-MAA reports were provided to the decision makers who owned the asset-specific risk, which is to say the private sector owners/operators. These reports were not wasted, as DCMA conducted follow-up reviews with the owners/operators. A number of anecdotes can give some sense of the fact that the reports did in fact provide for some improved resilience.

~~**PRE-DECISIONAL**~~
~~**FOR OFFICIAL USE ONLY**~~

~~PRE-DECISIONAL~~
~~FOR OFFICIAL USE ONLY~~

- ~~(FOUO)~~ OSD/JS: (b) (3), 10 USC § 130e
[REDACTED]
- ~~(FOUO)~~ OSD/JS: (b) (3), 10 USC § 130e
[REDACTED]
- ~~(FOUO)~~ OSD/JS: (b) (3), 10 USC § 130e
[REDACTED]
- ~~(FOUO)~~ OSD/JS: (b) (3), 10 USC § 130e
[REDACTED]
- ~~(FOUO)~~ OSD/JS: (b) (3), 10 USC § 130e
[REDACTED]
- ~~(FOUO)~~ OSD/JS: (b) (3), 10 USC § 130e
[REDACTED]
- ~~(FOUO)~~ OSD/JS: (b) (3), 10 USC § 130e
[REDACTED]
- ~~(FOUO)~~ OSD/JS: (b) (3), 10 USC § 130e
[REDACTED]
- ~~(FOUO)~~ OSD/JS: (b) (3), 10 USC § 130e
[REDACTED]

~~PRE-DECISIONAL~~
~~FOR OFFICIAL USE ONLY~~

~~PRE-DECISIONAL~~
~~FOR OFFICIAL USE ONLY~~

OSD/JS: (b) (3), 10 USC § 130e

- ~~(FOUO)~~ OSD/JS: (b) (3), 10 USC § 130e

- ~~(FOUO)~~ OSD/JS: (b) (3), 10 USC § 130e

Response to Review of Internal Controls Section

~~(FOUO)~~ The report states that ASD(HD&ASA) officials failed to maintain oversight of the DIB risk management process and failed to establish clear guidance for the DIB critical asset risk management process. A wide range of leadership activity going back at least to 2005 runs counter to this statement.

~~(FOUO)~~ OASD(HD&ASA) did maintain oversight of the risk management process through continual engagement, program reviews, and direct meetings between DASDs and PDs with DCMA and National Guard personnel. The Department has also had continued engagement on these issues driven both from GAO and Congressional staffer inquiries. The ASD(HD&ASA) has also testified to Congress on CIP issues related to the DIB. Specific guidance was provided to the DCMA Industrial Analysis Center through a DCMA/ASD(HD&ASA) Memorandum of Agreement giving specific direction. The Director of Mission Assurance and the DASD for Homeland Defense Strategy, Force Planning, and Mission Assurance continuously monitored this direction through the numerous program reviews of Industrial Analysis Center budget discussions. At one point in late 2010 the oversight reached such a detailed point of correction that DCMA leadership made targeted personnel moves within the program in order to respond to evolving understanding of mission assurance application within the DIB Sector.

~~(FOUO)~~ OASD(HD&ASA) recognized the resistance of the DIB to accept vulnerability assessments or share results early on and took steps to try and improve this relationship. This included high-level visits to DIB facilities and establishments of a DIB/CIP conference to create this increased trust environment. Once all these efforts proved unsuccessful in 2010, OASD(HD&ASA) recognized the futility of continuing DIB assessments and wound this effort down.

Finding: Defense Industrial Base Risk Management Process Requirements Not Met

~~PRE-DECISIONAL~~
~~FOR OFFICIAL USE ONLY~~

~~PRE-DECISIONAL~~
~~FOR OFFICIAL USE ONLY~~

~~(FOUO)~~ This finding is not accurate in the context of our evolving approach to risk management as discussed in the Risk Management Process Overview section above. While an earlier vision of interaction with the DIB private sector may have anticipated some DoD active intervention at individual assets, this is no longer the case. We have moved beyond this approach, and in accordance with our Mission Assurance Strategy, we will identify asset-based risks to DoD mission performance and manage those risks at the mission level.

~~(FOUO)~~ In one example the community surrounding a particular privately held DIB asset was greatly impacted by severe weather, with major infrastructure damage and loss of life. The Industrial Analysis Center engaged with the asset owner/operator to verify facility operations and track the impact of community losses on the asset. The Industrial Analysis Center cultivated continuous information flow and performed analysis of product inventory, production status, and reliability of deliveries. DoD maintained full ability to assess mission impact and conduct mission risk management if necessary.

Response to Insufficient Oversight of the Risk Management Process Section

~~(FOUO)~~ OASD(HD&ASA) maintained continuous engagement with DCMA regarding assessment scheduling and execution. This oversight permitted the Director, Mission Assurance to evaluate program capability and determine the inappropriate nature of the individual asset assessment approach. The table on page 7 of the draft report presents a data set that could potentially mislead uninformed readers. The table presents percentage data which implies a sudden program failure in 2010. In fact actual program performance was consistent, and as the program progressed from 2006 through 2010 the problematic nature of the original goals was clear. In particular the Director, Mission Assurance assessed the inability of DCMA to recruit sufficient asset owner/operator participation to accomplish the increased goals of 2010 and out-years. This data point should not be read as a failure of oversight but instead as an instance of management learning. This was critical to leadership decision to eliminate support for the individual asset assessment model.

Response to Policy for Risk Management Did Not Ensure Risks Were Assessed or Communicated Section

~~(FOUO)~~ This section takes two main tracks, first stating that DCMA did not perform and communicate results of risk assessments, and secondly that ASD(HD&ASA) did not provide appropriate guidance to DCMA in this matter. On the first issue, as indicated above, owners/operators are responsible for individual asset risk assessment. DCMA is responsible for analyzing DoD programmatic dependence on particular assets. Mission owners are responsible for the development of mission risk assessments, informed by the DCMA programmatic dependence analysis. The communication by DCMA with the mission owners has been on-going, and is continuously improving. It is also wrong to imply that because DCMA did not provide asset risk assessments then these were never done. Where a CIP-MAA has been done, the vast majority found that the owner/operator maintained a Business Continuity Plan, which in and of itself constitutes an asset risk assessment and mitigation plan.

~~PRE-DECISIONAL~~
~~FOR OFFICIAL USE ONLY~~

~~PRE-DECISIONAL~~
~~FOR OFFICIAL USE ONLY~~

~~(FOUO)~~ Also in the arena of communicating risk information, DoD is taking additional action above and beyond DCMA activities, further illustrating the fact that risk management activities go well beyond DCMA. The Sector Specific Plan identifies improved information sharing as a Goal. Recognizing that private sector owners/operators are the asset risk managers, DoD is expanding access to threat information. The DIB Cyber Security and Information Assurance Program provides cyber threat information directly to participating private sector partners. The Defense Security Service has initiated new paths of information flow to DIB owners/operators, while other elements of the defense intelligence enterprise have increased their attention to threats to DIB assets.

~~(FOUO)~~ On the second issue, while DCMA, as the tactical executor, did suggest much of the detailed approach in how they would execute their DISLA responsibilities, it is not correct to say they were responsible for writing their own program objectives. Rather, guided by the DoD issuances for DCIP, the Sector Specific Plan, and the DCMA/ASD(HD&ASA) Memorandum of Agreement, DCMA proposed various elements of their work plan in an iterative development, review, and finalization process with OSD(HD&ASA).

~~PRE-DECISIONAL~~
~~FOR OFFICIAL USE ONLY~~

Defense Contract Management Agency Comments



DEFENSE CONTRACT MANAGEMENT AGENCY

3901 A AVENUE BUILDING 10500

FORT LEE, VA 23801-1809

DEC 09 2011

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL
(ATTN: Ms. Amy L. Matthews, Program Director, Readiness,
Operations and Support)

SUBJECT: DCMA Review and Response to DoDIG Vulnerability and Risk Assessments
Needed to Protect Defense Industrial Base Critical Assets Report
(Project No. D2011-D000LA-0100.000)

In accordance with your request of December 8, 2011, DCMA has reviewed the Department of Defense Office of Inspector General Vulnerability and Risk Assessments Needed to Protect Defense Industrial Base Critical Assets report (Project No. D2011-D000LA-0100.000).

The Department of Defense Office of the Inspector General performed a review of the National and Defense Industrial Base (DIB) requirements and assessed DoD's execution of those policies. The draft report was issued on November 28, 2011 and recommended that the Director, Defense Contract Management Agency;

- a.) Conduct a review to ensure the Defense Contract Management Agency Industrial Analysis Center performs risk assessment on all DIB facilities that have vulnerability assessments.
- b.) Include in policy that vulnerability assessments should not be conducted on critical assets until threat and hazard information is available to complete a risk assessment.

DCMA concurs with recommendations and will schedule to obtain risk assessments prior to performing vulnerability assessments for any future assessments. The IAC also recommends concurrence with recommendation to develop internal procedures requiring threat and hazard assessments prior to performing any future assessments.

Questions may be addressed to [REDACTED]

Mr. Joseph E. Sweeney
Executive Director
Portfolio Management & Integration

~~FOR OFFICIAL USE ONLY~~



Inspector General
Department of Defense

~~FOR OFFICIAL USE ONLY~~