GAO Perspectives on the Assurance of Defense Critical Infrastructure

MORS Special Meeting on Optimizing Investments in Critical Infrastructure Protection

by

Davi M. D'Agostino
U.S. Government Accountability Office

Arlington, Virginia
November 17, 2010

For more information, contact Davi D'Agostino at
(202) 512-5431 or dagostinod@gao.gov

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
17 NOV 2010		**00-00-2010 to 00-00-2010**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
GAO Perspectives on the Assurance of Defense Critical Infrastructure	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Government Accountability Office,441 G Street NW,Washington,DC,20548**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Optimizing Investments in Critical Infrastructure Protection, 15?18 Nov 2010; ANSER Conference Center, Arlington, VA.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**23**	

Topics

- Overview of the U.S. Government Accountability Office (GAO)
- Defense Critical Infrastructure—Why Should We Be Concerned?
- DOD's Defense Critical Infrastructure Program (DCIP)
- Key Elements of the DCIP Risk Management Model
- Prior GAO Work
- Recent Congressional Concerns
- Electrical Power Risks and Vulnerabilities to DOD Critical Assets
- GAO Perspectives
- Selected GAO Recommendations
- Going Forward: Future Issues Surrounding the Assurance of Defense Critical Infrastructure
- Related GAO Products

GAO—Who Are We?

- GAO is an independent, nonpartisan professional services agency in the Legislative Branch of the Federal Government.
- GAO supports the Congress in meeting its constitutional responsibilities and to help improve the performance and ensure the accountability of the federal government for the benefit of the American people.
- Commonly known as the "**audit and investigative arm of the Congress**" or the "**congressional watchdog**," GAO examines how taxpayer dollars are spent; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help the Congress make informed oversight, policy, and funding decisions.
- GAO provides the Congress with timely information that is **objective**, **fact-based**, **nonpartisan**, **nonideological**, **fair**, and **balanced**.

Defense Critical Infrastructure—Why Should We Be Concerned?

- DOD relies on a global network of defense critical infrastructure so essential that the incapacitation, exploitation, or destruction of an asset within this network could severely affect DOD's ability to deploy, support, and sustain its forces and operations worldwide and to implement its core missions, including those in Iraq and Afghanistan as well as its homeland defense and strategic missions.
- DOD's **most critical infrastructure assets**—assets of such extraordinary importance to DOD operations that their incapacitation or destruction would have a very serious, debilitating effect on the ability of the department to fulfill its missions—include both DOD- and non-DOD-owned assets located both within the United States and abroad.
- Overall, about 85 percent of the infrastructure DOD relies on is owned by non-DOD entities (e.g., private industry and foreign commercial entities and governments).

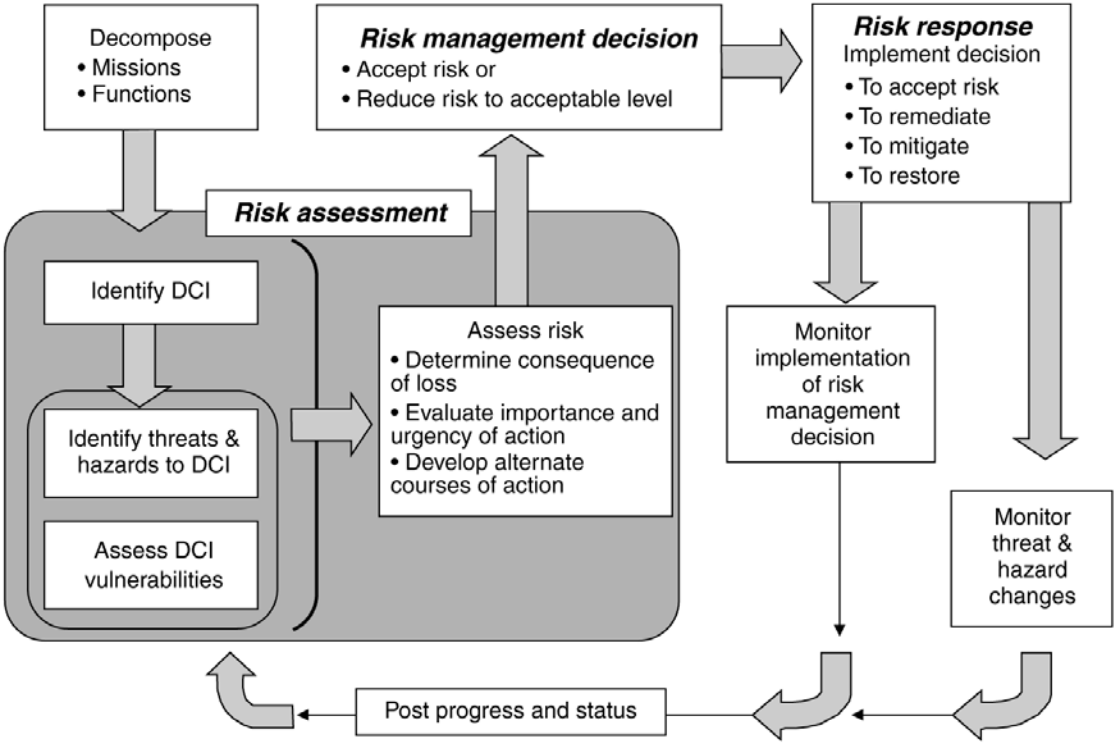
DOD's Defense Critical Infrastructure Program (DCIP)

- In 2005, DOD established DCIP to identify and assure the availability of mission-critical infrastructure.
  - DCIP encompasses the full spectrum of threats—ranging from terrorist attacks to natural disasters and catastrophic accidents—that can adversely affect critical infrastructure.
  - DOD assigned overall DCIP responsibility to the Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (ASD(HD&ASA)).

DOD's Defense Critical Infrastructure Program (DCIP) (cont'd)

- DOD can also assess risk and vulnerabilities to its critical infrastructure through other mission assurance programs and efforts:
  - Force protection.
  - Antiterrorism.
  - Defense continuity.
  - Information assurance.
  - Continuity of operations.
  - Chemical, biological, radiological, nuclear, and high-explosive defense.
  - Readiness.
  - Installation preparedness.
- Within *National Infrastructure Protection Plan* framework, DOD collaborates with DHS and DOE to address electrical power infrastructure risks and vulnerabilities.

Key Elements of the DCIP Risk Management Model



Source: DOD Instruction 3020.45.

- DOD's program is designed to identify the vulnerabilities of and manage the risks to its most critical assets primarily through DCIP.

Key Elements of the DCIP Risk Management Model (cont'd)

- To ensure the availability of assets critical to DOD missions, DCIP uses a risk management model that helps decision makers
  - identify the department's critical assets based on the criticality of their missions;
  - conduct "threat and hazard assessments;"
  - conduct "vulnerability assessments" (that include detailed reviews of electrical power vulnerabilities);
  - conduct "risk assessments" to determine the consequences of the assets' loss, evaluate the importance and urgency of proposed actions, and develop alternate courses of action;
  - reach "risk management decisions" to accept risks or reduce risks to acceptable levels; and
  - formulate "risk responses" to implement the risk management decisions.

Prior GAO Work

- Since 2007, GAO has conducted an extensive body of work in response to congressional requests on DOD's efforts to assure the availability of defense critical infrastructure, and issued 10 reports containing 44 recommendations on
  - DOD's progress in addressing the evolving management framework for DCIP;
  - coordination among DCIP stakeholders;
  - implementation of key program elements;
  - DCIP funding;
  - actions DOD has taken to assure the availability of critical infrastructure in five defense sectors (the Defense Industrial Base; Global Information Grid; Intelligence, Surveillance, and Reconnaissance; Space; and Transportation);
  - consistency, reliability, and usefulness of DOD's critical asset list;
  - highly sensitive assets;
  - training standards; and
  - the identification and management of electrical power risks and vulnerabilities to DOD critical assets.
- GAO has also issued related reports concerning federal critical infrastructure protection, cyber security, and electrical power.

Recent Congressional Concerns

- Most recently, the House Committee on Armed Services expressed concerns about electrical power disruptions to critical DOD missions.
- Committee mandated that GAO review the assurance of electrical power supplies to DOD installations with critical assets and examine the extent to which
  - DOD's most critical assets are vulnerable to disruptions in electrical power supplies and
  - DOD—both within and outside DCIP—has attempted to assure the availability of electrical power supplies to its most critical assets.
- GAO issued a report on *Defense Critical Infrastructure: Actions Needed to Improve the Identification and Management of Electrical Power Risks and Vulnerabilities to DOD Critical Assets.* GAO-10-147. Washington, D.C.: October 23, 2009.

Electrical Power Risks and Vulnerabilities to DOD Critical Assets

- DOD relies overwhelmingly on commercial electrical power grids for secure, uninterrupted electrical power to support its critical assets.
- In 2008, the Defense Science Board reported that “[c]ritical national security and homeland defense missions are at an unacceptably high risk of extended outage from failure of the [commercial electrical power] grid.”

Electrical Power Risks and Vulnerabilities to DOD Critical Assets (cont'd)

- Reliability and security of commercial electrical power grids are increasingly threatened by a convergence of challenges:
  - Increased user demand.
  - An aging electrical power infrastructure.
  - Increased reliance on automated control systems that can be susceptible to cyber attack.
  - The attractiveness of electrical power infrastructure for terrorist attacks.
  - Long lead times for replacing key electrical power equipment.
  - More frequent interruptions in fuel supplies to electricity-generating plants.
- As a result, commercial electrical power grids have become increasingly fragile and vulnerable to extended disruptions that could severely impact DOD's most critical assets, their supporting infrastructure, and ultimately the missions they support.
- All of DOD's most critical assets require electricity continuously to support their military missions.
  - Almost all of them rely on commercial power grids—which are increasingly fragile and vulnerable—as their primary source of electricity.

GAO Perspectives: Status of DOD's Vulnerability Assessments of Its Most Critical Assets

- DOD is required to conduct vulnerability assessments on all its most critical assets at least once every 3 years.
- As of October 2010, DOD had conducted DCIP vulnerability assessments on almost all of its most critical assets that were identified in October 2008.
- At the time of our review, DOD had neither conducted, nor developed additional guidelines and time frames for conducting, these vulnerability assessments on any of the non-DOD-owned most critical assets located in the United States or foreign countries, citing security concerns and political sensitivities.
- DOD does not systematically coordinate DCIP vulnerability assessment processes and guidelines with those of other, complementary DOD mission assurance programs that also examine electrical power vulnerabilities of the most critical assets; however, DOD is in the process of developing guidelines for such systematic coordination.
- The 10 DCIP vulnerability assessments we reviewed did not consider assets' vulnerabilities to longer-term (i.e., of up to several weeks' duration) electrical power disruptions on a mission-specific basis.

GAO Perspectives: DOD Lacks Sufficient Information to Determine Full Extent of Power Grid Vulnerabilities

- With more comprehensive knowledge of the most critical assets' vulnerabilities to electrical power disruptions, DOD can better avoid compromising crucial missions due to electrical power disruptions.
- Additional information on power grid vulnerabilities should improve DOD's ability to effectively prioritize funding needed to address them vis-à-vis DOD's most critical assets and better work with DHS and the private sector.

GAO Perspectives: DOD Has Taken Some Steps Toward Assuring the Availability of its Electrical Power Supplies to Its Most Critical Assets

- From August 2005 through October 2008, DOD issued DCIP guidance for identifying critical assets, assessing their vulnerabilities, and making risk management decisions about those vulnerabilities.
- DOD has conducted various types of vulnerability assessments—including DCIP vulnerability assessments, Joint Staff Integrated Vulnerability Assessments, and other mission assurance–related assessments—on about 70 percent of its most critical assets, including multiple assessments on some of the same assets.
  - These vulnerability assessments have identified various electrical power vulnerabilities for about 30 percent of the assets.
- DOD has also coordinated with DHS, DOE, and the Federal Energy Regulatory Commission and industry organizations in an effort to assure the availability of electrical power supplies to its critical assets.

GAO Perspectives: DOD Has Taken Some Steps Toward Assuring the Availability of its Electrical Power Supplies to Its Most Critical Assets (cont'd)

- DOD participates in the Energy Government Coordinating Council, which provides a forum at the infrastructure sector level for sharing concerns on energy-related matters—including critical infrastructure protection—with DOE.
  - ✓ However, DOD coordination with DHS at the (energy) sector level is not at a level in which DHS could help DOD address individual installation/asset-related priorities, dependencies, and vulnerabilities.
- U.S. European Command and U.S. Africa Command have agreed to accept a DOE energy attaché to provide energy-related expertise on the security and reliability of the commands' energy infrastructure.
- DOD serves as co-chair of the federal Task Force on Electric Grid Vulnerability of the National Science and Technology Council's Committee on Homeland and National Security, which identify research and development needs for electrical grid vulnerabilities and to coordinate with other federal agencies.
- Full coordination and information sharing with private-sector and foreign commercial entities and governments on critical assets is problematic because DOD's list of its most critical assets is highly classified.

GAO Perspectives: DOD Lacks a Mechanism for Tracking the Implementation of Future DCIP Risk Management Decisions and Responses

- ASD(HD&ASA)—which has responsibility for overseeing the implementation of actions for the remediation, mitigation, or acceptance of risks to DOD critical assets—has not yet developed a mechanism to track the
  - implementation of future DCIP risk management decisions and
  - responses (i.e., remediation, mitigation, and risk acceptance actions that may require funding) intended to address risks and vulnerabilities identified for the most critical assets.
- Without such information, DOD cannot determine with any certainty whether asset owners are taking the necessary steps to address identified risks and vulnerabilities of its most critical assets to electrical power disruptions.

GAO Perspectives: DOD Coordination with Local Electricity Providers Has Been Limited

- DCIP guidance encourages coordination between DOD installations with critical assets and their respective public utilities, including electricity providers, to remediate risks involving those utilities.
- We found that such coordination with local electricity providers has occurred for only about 20 percent of DOD's most critical assets.
- As a result, DOD may not be taking advantage of available expertise on electrical power issues from such providers.
- Without increased coordination between more DOD installations with critical assets and their respective local electricity providers, DOD limits the risk mitigation and remediation options available for addressing electrical power disruptions.

Selected GAO Recommendations

- GAO recommended, in part, that DOD:
  - Complete DCIP vulnerability assessments on all DOD-owned most critical assets.
  - Develop additional guidelines, an implementation plan, and a schedule for conducting such assessments on all non-DOD-owned most critical assets.
  - Finalize guidelines to coordinate DCIP assessment criteria and processes with those of other DOD mission assurance programs.
  - Develop DCIP guidelines for assessing the most critical assets' vulnerabilities to longer-term electrical power disruptions.
  - Develop a mechanism to track the implementation of future DCIP risk management decisions.
  - Ensure or facilitate coordination between asset owners and host installations of the most critical assets and to local electricity providers to remediate and mitigate risks and vulnerabilities to electrical power disruptions.
- DOD concurred with all of GAO's recommendations and is implementing them.

Going Forward: Future Issues Surrounding the Assurance of Defense Critical Infrastructure

- Disconnect created because mission owners often are not critical infrastructure asset owners or the bill payers.
- Redundancy in DOD's mission assurance programs.
- Assurance of DOD's cyber-based critical infrastructure.
- Protecting the Defense Industrial Base from cyber threats.
- Using Smart Grid–related technologies, which may introduce additional vulnerabilities to the U.S. electrical power grid, such as increased susceptibility to cyber attacks.
- Interoperability and continuity of operations for DOD's global information grid.
- Assurance of non-DOD-owned defense critical infrastructure at home and abroad.
- Protecting against electromagnetic pulse attacks on defense critical infrastructure.

Related GAO Products

- *Defense Critical Infrastructure: Actions Needed to Improve the Identification and Management of Electrical Power Risks and Vulnerabilities to DOD Critical Assets.* GAO-10-147. Washington, D.C.: October 23, 2009.
- *Defense Critical Infrastructure: Actions Needed to Improve the Consistency, Reliability, and Usefulness of DOD's Tier 1 Task Critical Asset List*. GAO-09-740R. Washington, D.C.: July 17, 2009.
- *Defense Critical Infrastructure: Developing Training Standards and an Awareness of Existing Expertise Would Help DOD Assure the Availability of Critical Infrastructure*. GAO-09-42. Washington, D.C.: October 30, 2008.

Related GAO Products (cont'd)

- *Defense Critical Infrastructure: Adherence to Guidance Would Improve DOD's Approach to Identifying and Assuring the Availability of Critical Transportation Assets*. GAO-08-851. Washington, D.C.: August 15, 2008.
- *Defense Critical Infrastructure: DOD's Risk Analysis of Its Critical Infrastructure Omits Highly Sensitive Assets*. GAO-08-373R. Washington, D.C.: April 2, 2008.
- *Defense Infrastructure: Management Actions Needed to Ensure Effectiveness of DOD's Risk Management Approach for the Defense Industrial Base*. GAO-07-1077. Washington, D.C.: August 31, 2007.
- *Defense Infrastructure: Actions Needed to Guide DOD's Efforts to Identify, Prioritize, and Assess Its Critical Infrastructure*. GAO-07-461. Washington, D.C.: May 24, 2007.

GAO on the Web

Web site: http://www.gao.gov/

Contact

Chuck Young, Managing Director, Public Affairs, youngc1@gao.gov
(202) 512-4800, U.S. Government Accountability Office
441 G Street NW, Room 7149, Washington, D.C. 20548

Copyright