



Department of Homeland Security Office of Inspector General

DHS Risk Assessment Efforts in the Dams Sector





**Homeland
Security**

SEP 15 2011

Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the Department.

This report addresses the strengths and weaknesses of the Office of Infrastructure Protection's efforts to assess risk to critical infrastructure under a voluntary framework. It is based on interviews with employees and officials of relevant agencies and institutions, direct observations, and a review of applicable documents.

The recommendation herein has been developed to the best knowledge available to our office, and has been discussed in draft with those responsible for implementation. We trust this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

A handwritten signature in black ink, reading "Anne L. Richards".

Anne L. Richards

Assistant Inspector General for Audits

Table of Contents/Abbreviations

Executive Summary	1
Background	2
Results of Audit	3
Review of Risk Assessments	4
Security Reviews for Critical Dam Assets	4
Mitigation of Identified Security Risks	5
Conclusion	6
Recommendation	6
Management Comments and OIG Analysis	6

Appendices

Appendix A: Purpose, Scope, and Methodology	8
Appendix B: Management Comments to the Draft Report	10
Appendix C: Major Contributors to this Report	13
Appendix D: Report Distribution	14

Abbreviations

DHS	Department of Homeland Security
FY	fiscal year
IP	Office of Infrastructure Protection
OIG	Office of Inspector General



Department of Homeland Security
Office of Inspector General

Executive Summary

The protection of the Nation's critical infrastructure is one of the primary missions of the Department of Homeland Security. The National Infrastructure Protection Plan provides the strategy to organize and carry out the national effort to protect 18 sectors of critical infrastructure, one of which is the Dams Sector. Dams and related structures are especially important because one catastrophic failure at some locations could affect populations exceeding 100,000 and have economic consequences surpassing \$10 billion.

The purpose of our review was to determine whether the Office of Infrastructure Protection and other components of the Department have taken steps to assess risk at the most critical dam assets, and followed up to ensure that recommendations were implemented.

The Department lacks assurance that risk assessments were conducted and that security risks associated with critical dam assets were identified and mitigated. The Department did not:

- Review all critical dam asset risk assessments conducted by other agencies,
- Conduct security reviews for 55% of the critical dam assets, or
- Ensure that corrective actions were completed to mitigate risk when security gaps were identified.

The Department was unable to complete these tasks because it does not have the necessary authority to ensure that security partners participate in risk management activities, or that dam owners/operators undergo departmental assessments and implement corrective action.

We are making one recommendation to the Office of Infrastructure Protection that, when implemented, will improve the Department's efforts to secure the Dams Sector.

Background

Protecting the Nation's critical infrastructure is one of the primary missions of the Department of Homeland Security (DHS). In December 2003, Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection*, established U.S. policy to enhance the protection of the critical infrastructure and key resources of the United States. It tasked the Secretary of DHS with coordinating the overall national effort and serving as the principal federal official to lead, integrate, and coordinate federal departments and agencies implementing the policy.

The directive identified critical infrastructure sectors and designated federal Sector-Specific Agencies to encourage risk management strategies to protect against and mitigate the effects of attacks against critical infrastructure and key resources. "Sectors" are logical collections of assets, systems, or networks that provide a common function to the economy, government, or society. Homeland Security Presidential Directive 7 established 17 such sectors (with the 18th sector, Critical Manufacturing, added later). The directive also assigned responsibility for individual sectors to federal Sector-Specific Agencies. The DHS Office of Infrastructure Protection (IP) is the Sector-Specific Agency for the Dams Sector.

The Dams Sector consists of dams, navigation locks, levees, and other similar water retention and control facilities, collectively known as "dam assets." In fiscal year (FY) 2009, DHS identified several hundred critical dam assets through the National Critical Infrastructure Prioritization Program. This program, implemented by IP, conducts an annual data call to the State Homeland Security Advisors and Sector-Specific Agencies to identify infrastructure that "would, if destroyed or disrupted, cause national or regional catastrophic effects."

These critical dam assets are owned by private entities, federal agencies, and state and local governments. Dam assets are regulated by a variety of entities. For example, state dam safety offices regulate some dams; federal agencies that own and operate dams, such as the U.S. Army Corps of Engineers, are self-regulating; and the Federal Energy Regulatory Commission regulates most hydroelectric facilities.

Homeland Security Presidential Directive 7 mandated the development of a National Plan for Critical Infrastructure and Key Resources Protection to integrate critical infrastructure protection

efforts by governments, the private sector, international organizations, and foreign governments into a single national program. The first National Infrastructure Protection Plan was released in 2006. The National Infrastructure Protection Plan development and support is carried out within a largely voluntary partnership framework. The National Infrastructure Protection Plan includes the Critical Infrastructure Partnership Advisory Council, a legal framework to organize the asset owners, operators, and federal, state, local, and tribal government entities in sector planning, collaboration, and information sharing. An outcome of this partnership is the development of Sector-Specific Plans.

As the Sector-Specific Agency for dams, IP's responsibilities include identifying, assessing, and prioritizing dam sector assets. The IP's Dams Branch is responsible for sector-wide risk assessments. To accomplish its goals, IP partners with the Bureau of Reclamation, U.S. Army Corps of Engineers, Federal Energy Regulatory Commission, Federal Emergency Management Agency, and state governments.

Results of Audit

DHS lacks assurance that risk assessments were conducted and security risks associated with critical dam assets were identified and mitigated. Specifically, the Department did not:

- Review all critical dam asset risk assessments conducted by other agencies,
- Conduct security reviews for 55% of the critical dam assets as of March 2011 to assess their overall security posture, or
- Ensure that corrective actions were completed to mitigate risk when security gaps were identified.

DHS was unable to complete these tasks because it does not have the authority to ensure that security partners participate in risk management activities or that dam owners undergo departmental assessments and implement corrective action. The National Infrastructure Protection Plan prescribes a partnership approach between government and the private sector to voluntarily manage risk. Underlying legislation does not give the Department the necessary authority to ensure that security partners participate in risk management activities, or that dam owners undergo departmental assessments and implement corrective action. DHS could not always obtain cooperation from its security partners and dam owners, and did not always collaborate successfully. This collaborative approach can succeed only if security partners and dam owners work together to perform risk management.

Review of Risk Assessments

IP cannot determine whether security risks at critical dam assets have been identified and mitigated because it has not obtained and reviewed the adequacy of risk assessments at critical assets. As a result, IP does not know whether all critical dam assets have undergone risk assessments, or the quality of those that were performed. IP contends that its federal partners do review asset-specific security risk assessments in accordance with well-established internal directives and policies. However, it indicated that it does not have the authority to require official evidence of such reviews to be provided under the National Infrastructure Protection Plan's voluntary framework. Unless DHS verifies the existence and quality of the risk assessments, IP cannot ensure that critical dam assets are protected.

Security Reviews for Critical Dam Assets

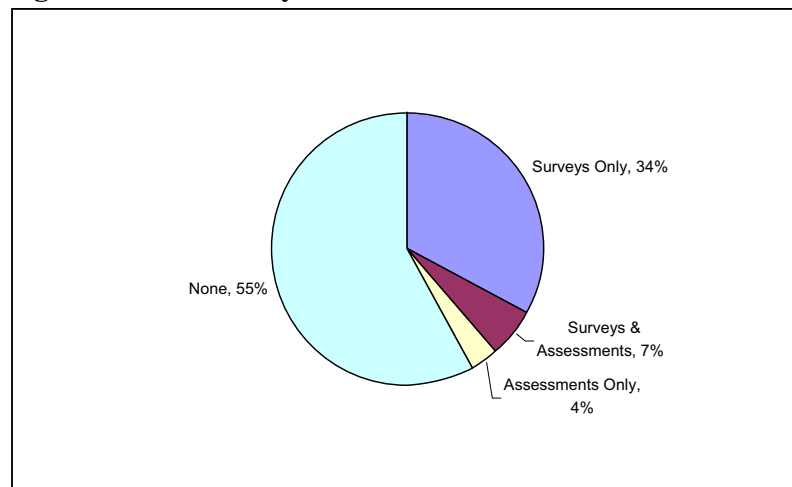
IP has conducted security reviews for only 45% of the critical dam assets to assess their overall security posture. IP does not know the security posture for the remaining 55% of the critical dam assets.

For IP to conduct a security review, the owner/operator must voluntarily collaborate with IP. Two types of security assessments conducted by IP are Enhanced Critical Infrastructure Protection Security Surveys and Site Assistance Visits.

- Enhanced Critical Infrastructure Protection Security Surveys involve a survey of assets of national significance, based primarily on a questionnaire completed through an interview, or a partial or full site review. Information is obtained on a facility's security force, physical security, access controls, and surveillance and detection capabilities.
- Site Assistance Visits are non-regulatory risk-informed vulnerability assessments that assist an owner or operator with identifying and documenting critical infrastructures, vulnerabilities, protective measures, planning needs, and options for consideration to increase protection from, and resilience to, a wide range of hazards.

Figure 1 illustrates IP's assessment of assets identified during the FY 2009 National Critical Infrastructure Prioritization Program.

Figure 1. IP Security Reviews



Source: Office of Inspector General (OIG) analysis of IP reviews.

We reviewed 94% of the IP-completed survey questionnaires and found that 47% of the asset owners were not completing vulnerability assessments, not sharing vulnerability assessments with DHS, or not implementing “options for consideration” from the vulnerability assessments. The term “vulnerability assessments” has been used interchangeably with risk assessments and includes a wide range of risk and vulnerability assessment methodologies used by security partners in the Dams Sector. Unless IP verifies the existence and quality of the risk assessments, it cannot ensure that critical dam assets are protected.

According to one IP Protective Security Advisor, dam owners and operators tend to be more concerned with daily operations than with preparing for possible future catastrophes; unless an asset’s regulatory agency requires a vulnerability assessment, it likely will not be done. Protective Security Advisors said that some asset operators did not have the authority to release the results of vulnerability assessments. Although IP could have requested these vulnerability assessments through the asset owners’ regulatory agencies, it chose not to do so in the instances reviewed.

Mitigation of Identified Security Risks

Our review of IP-completed survey questionnaires revealed gaps in security controls at critical dam assets. Similarly, our review of the IP-completed site assistance visits at critical dam assets identified numerous security gaps. When DHS personnel identify security weaknesses during site assistance visits, they provide the owner with “Options for Consideration,” which are corrective actions designed to mitigate the security risks. However, implementation of the corrective actions is at the discretion of the facility owner because the Department

has no regulatory authority over the dams. As such, DHS cannot enforce its recommendations.

In contrast to the Dams Sector, which operates outside of DHS' regulatory reach, the *Department of Homeland Security Appropriations Act of 2007* provided DHS with the authority to regulate the security of high-risk chemical facilities. Section 550 of the act requires the Secretary of DHS to promulgate interim final regulations "establishing risk-based performance standards for security of chemical facilities" that the Secretary determines present high levels of security risk. The act and its implementing regulations mandate audits and inspections to determine compliance with the regulations, provide for civil penalties for violation of an order issued under the act, and allow the Secretary to order a facility to cease operations if it is not in compliance with the requirements.¹

Conclusion

The absence of security reviews, combined with the inability to require asset owners to mitigate security vulnerabilities when assessments are conducted, has prevented the Department from identifying and mitigating security risks. DHS needs authority to review risk assessments, conduct inspections when assessments are deficient, and make recommendations for corrective actions.

Recommendation

We recommend that the Assistant Secretary, Office of Infrastructure Protection:

Recommendation #1: Determine the appropriateness of a legislative proposal to establish regulatory authority for the critical Dams Sector assets similar to the Chemical Sector. Specifically, DHS personnel need authority to review risk assessments, conduct inspections when assessments are deficient, and make recommendations for corrective actions.

Management Comments and OIG Analysis

In its response to the draft report, the National Protection and Programs Directorate/Office of Infrastructure Protection provided additional information regarding the specific agency responsibilities involved within a voluntary framework. The Directorate noted that criteria for determining critical assets were recently refined, resulting in a lower number of critical assets and a corresponding increase in the percentage of

¹ Implementing regulations for Section 550 of the Department of Homeland Security Appropriations Act of 2007 are at Title 6 of the Code of Federal Regulations, Part 27.

assets assessed by the Directorate. As many agencies at the federal and state level oversee the safety and security of dams, the robustness of security programs varies greatly, as it is directly influenced by regulatory agency level of authority and available resources. Finally, the Directorate noted that voluntary implementation of options for consideration to owners and operators are presented to illustrate the benefits of such improvements, rather than providing top-down management as a regulatory authority might do.

The Directorate concurred with the recommendation to determine the appropriateness of a legislative proposal. The Directorate is beginning work and research to make that determination and a subsequent recommendation for action. As part of the continuous review of the effectiveness of the partnership framework, this analysis will provide insight into new programs and refinements of current initiatives needed to address any critical gaps. The Directorate will coordinate with internal DHS stakeholders, including the Offices of General Counsel and Legislative Affairs, and representatives from federal and state agencies currently responsible for the regulation of critical Dams Sector assets, as part of its analysis of the appropriateness of a legislative proposal.

We agree that the planned corrective action adequately addresses the recommendation. However, the recommendation will remain open and unresolved until a target date for completion of the analysis is provided.

Appendix A

Purpose, Scope, and Methodology

The purpose of our review was to determine whether IP and other components of the Department have identified and taken steps to assess risk at the most critical dam assets, and followed up to ensure that recommendations were implemented.

We met with divisional offices within IP under the DHS Directorate for National Protection and Programs, including the Sector-Specific Agency Executive Management Office, Protective Security Coordination Division, Infrastructure Analysis & Strategy Division, and the Infrastructure Information Collection Division. We also interviewed security partners, including the Bureau of Reclamation; U.S. Army Corps of Engineers; Federal Energy Regulatory Commission; Federal Emergency Management Agency; and the states of Maryland, New Jersey, New York, Tennessee, and Texas.

We reviewed relevant Government Accountability Office and OIG reports, the *Homeland Security Act of 2002*, *Critical Infrastructure Information Act of 2002*, *Post-Katrina Emergency Management Reform Act of 2006*, *Implementing Recommendations of the 9/11 Commission Act of 2007*, Homeland Security Presidential Directive 7, National Infrastructure Protection Plan, and the Dams Sector-Specific Plan. We obtained minutes from selected meetings between June 2007 and November 2009 of the Dams Sector Joint Government Coordinating Council and the Sector Coordinating Councils as part of the Critical Infrastructure Partnership Advisory Council.

We reviewed IP Enhanced Critical Infrastructure Protection Security Surveys and Site Assistance Visits to determine the security weaknesses at the critical dam assets. We contacted other infrastructure sectors to understand the processes they used in assessing risk within their respective sectors. We also contacted members of the Sector Coordinating Council to understand the concerns of the private sector in assessing and mitigating risks at their facilities.

We examined regulations issued by DHS that apply to high-risk chemical facilities. We also compared risk-based performance standards at high-risk chemical facilities with existing security controls at critical dam assets.

We conducted this performance audit between January 2010 and March 2011 pursuant to the *Inspector General Act of 1978*, as amended, and according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to

Appendix A
Purpose, Scope, and Methodology

provide a reasonable basis for our findings and conclusions based upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives.

Appendix B

Management Comments to the Draft Report

Office of the Under Secretary
National Protection and Programs Directorate
U.S. Department of Homeland Security
Washington, DC 20528



**Homeland
Security**

JUL 20 2011

Anne L. Richards
Assistant Inspector General for Audits
Office of Inspector General
U.S. Department of Homeland Security
Washington, DC 20528

Dear Ms. Richards:

Re: OIG Project No. 10-002-AUD-DHS, *DHS Risk Assessment Efforts in the Dams Sector*

The Department of Homeland Security (DHS)/National Protection and Programs Directorate (NPPD) appreciates the opportunity to review and respond to the Office of Inspector General (OIG) draft report OIG Project No. 10-002-AUD-DHS, *DHS Risk Assessment Efforts in the Dams Sector*. This audit was conducted to determine whether the Office of Infrastructure Protection (IP) and other components of the Department have (1) taken steps to assess risk at the most critical dam assets and (2) followed up to ensure that owners and operators have implemented recommendations. NPPD and IP are working to resolve the issues identified in the report.

The OIG report presents an evaluation of risk assessment efforts associated with these critical assets. We provide the following information to augment their discussion and provide a more comprehensive picture of the current landscape of risk assessment efforts in the Dams Sector, including

- risk assessment responsibilities of DHS as the Dams Sector-Specific Agency (SSA) and lead for the overall national effort to enhance critical infrastructure protection;
- updated data since fieldwork was completed;
- the current regulatory framework; and
- our efforts to have asset owners voluntarily follow up on options for consideration.

First, DHS and SSA responsibilities with respect to risk assessments include “coordinating, facilitating, and supporting comprehensive risk assessment and risk management programs” for high-risk assets and systems.¹ In a voluntary framework, DHS does this through conducting voluntary vulnerability assessments and security surveys on critical infrastructure at the owner/operators’ request, supporting other

¹ U.S. Department of Homeland Security, National Infrastructure Protection Plan, 2009: p. 17.

Appendix B

Management Comments to the Draft Report

Federal, State, local, tribal, and territorial partners in their assessments as requested, and conducting risk analysis on the sector as a whole. The SSA also provides valuable tools to the private sector owners and operators to allow them to do their own facility-level assessments.

Second, the OIG report is based on the facilities identified as critical through the Fiscal Year (FY) 2009 National Critical Infrastructure Prioritization Program (NCIPP) data call. The NCIPP criteria were significantly refined after FY 2009. Consequently, the total number of dams deemed critical has decreased, and the percentages of assets assessed by NPPD/IP have increased.

Third, a number of different agencies at the Federal and State levels of government oversee the safety and security of dams. Considering the most recent data, most (approximately 80 percent) of critical dam assets in the FY 2011 NCIPP list are owned, operated, and/or regulated by Federal agencies, such as the U.S. Army Corps of Engineers, U.S. Bureau of Reclamation, U.S. International Boundary and Water Commission, Tennessee Valley Authority, and Federal Energy Regulatory Commission. These agencies have robust programs for identifying critical assets, completing facility-level security risk assessments, determining the necessary level of protection, implementing security programs, and/or assessing performance. The remaining assets in the FY 2011 NCIPP list fall under the jurisdiction of State agencies which, in most cases, have regulatory responsibility over dam safety issues. The robustness of the dam security programs implemented by these State regulatory agencies is directly influenced by their level of authority and available resources, which is quite varied.

Fourth, DHS and SSA engagement with the Dams Sector is conducted in a voluntary framework—there is no associated enforcement authority. Within this voluntary framework, we believe it is important to work as partners with our stakeholders. NPPD/IP presents the voluntary implementation of options for consideration to owners and operators as a business case, illustrating the benefits such improvements would have for operations of that facility, rather than providing top down management as an organization with regulatory authority might do. NPPD/IP is currently expanding and refining a new voluntary program to follow up on actions taken after our assessments. So far, the program is well received by the Dams Sector.

OIG Recommendation

The OIG recommended that the Assistant Secretary, Office of Infrastructure Protection, determine the appropriateness of a legislative proposal to establish regulatory authority for the critical Dams Sector assets similar to the Chemical Sector. The OIG clarified that such regulatory authority would grant DHS personnel authority to review risk assessments, conduct inspections when assessments are deficient, and make recommendations for corrective actions. NPPD/IP concurs with the recommendation to determine the appropriateness of a legislative proposal, and we are beginning work and research to make that determination and a subsequent recommendation.

Appendix B

Management Comments to the Draft Report

As part of the continuous review of the effectiveness of the partnership framework, this analysis will provide insight into new programs and refinements of current initiatives needed to address any critical gaps. NPPD/IP will coordinate with internal DHS stakeholders, including the Offices of General Counsel and Legislative Affairs, and representatives from Federal and State agencies currently responsible for the regulation of critical Dams Sector assets as part of its analysis of the appropriateness of a legislative proposal.

Again, we thank you for the opportunity to review and provide comment on this draft report, and look forward to working with you on future homeland security engagements.

Sincerely,



Rand Beers
Under Secretary

Attachments

- 1) Sensitivity Review
- 2) Technical comments

Appendix C

Major Contributors to this Report

Michael Sivi, Director
Dennis Deely, Audit Manager
Kevin Donahue, Auditor
Anthony Colache, Program Analyst
Ebenezer Jackson, Program Analyst
Ashley Smith, Program Analyst
Kathleen Hyland, Referencer

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretariat
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Under Secretary for National Protection and Programs Directorate
Assistant Secretary for Office of Infrastructure Protection
Director, GAO-OIG Audit Liaison Office for the National
Protection and Programs Directorate

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as
appropriate



ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4305, or visit the OIG web site at www.dhs.gov/oig.

OIG HOTLINE

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations:

- Call our Hotline at 1-800-323-8603;
- Fax the complaint directly to us at (202) 254-4292;
- Email us at DHSOIGHOTLINE@dhs.gov; or
- Write to us at:
DHS Office of Inspector General/MAIL STOP 2600,
Attention: Office of Investigations - Hotline,
245 Murray Drive, SW, Building 410,
Washington, DC 20528.

The OIG seeks to protect the identity of each writer and caller.