U.S. Department of the Interior
Office of Inspector General

ADVISORY LETTER

Department of the Interior Responses to Review Guide for Planning and Assessment Activities for Protecting Critical Non-Cyber Infrastructures

No. 2002-I-0012 DECEMBER 2001

United States Department of the Interior

Office of Inspector General
Washington, D.C. 20240

December 21, 2001

Advisory Letter

Memorandum

To: Assistant Secretary for Policy, Management and Budget

From: Elaine T. Weistock
Director, Quality Assurance and Audit Followup

Subject: Advisory Letter on Department of the Interior Responses to Review Guide for Planning and Assessment Activities for Protecting Critical Non-Cyber Infrastructures (No. 2002-I-0012)

As requested by the President's Council on Integrity and Efficiency (PCIE), we completed the PCIE's review guide, which was designed to obtain information concerning the critical physical infrastructure and planning processes used by the Department of the Interior (DOI). We conducted the review as part of a Governmentwide four-phase PCIE evaluation of Federal agency implementation of Presidential Decision Directive 63 (PDD-63). The Directive called for a national effort to ensure the security of the Nation's critical physical and cyber-based infrastructures.[1] The four phases of the review include the following:

- Agency planning and assessment activities for protecting critical cyber-based infrastructures (Phase I).
- Agency implementation activities for protecting cyber-based infrastructures (Phase 2).
- Agency planning and assessment activities for protecting critical non-cyber infrastructures (Phase 3).
- Agency implementation activities for protecting critical non-cyber infrastructures (Phase 4).

We also evaluated DOI's implementation of the two recommendations contained in our Phase 1 advisory letter (No. 00-I-704), which was issued in September 2000. The results of the review will be sent to the PCIE working group for inclusion in a Governmentwide report concerning the security of Federal Critical Infrastructures.

[1]Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and Government, including, but not limited to, telecommunications, energy, banking and finance, transportation, and water systems and emergency services, both Governmental and private.

Background

Advances in information technology have resulted in increasing the automation and interlinking of physical and cyber-based infrastructures and have created new vulnerabilities to intentional or unintentional infrastructure attacks from human error, weather, and equipment failure that could significantly harm the Nation's economy and military capability.

PDD-63, signed on May 22, 1998, ordered the strengthening of the Nation's defense against terrorist acts, weapons of mass destruction, and assaults on critical infrastructures that would diminish the ability of the Government to protect the national security and ensure general public health and safety; the state and local governments to maintain order and deliver minimum essential public services; and the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial, and transportation services. PDD-63 directs the Government to eliminate any significant vulnerability to both physical and cyber attacks on its critical infrastructures by May 22, 2003.

DOI's Critical Infrastructure Protection Plan (CIPP) identified Hoover Dam, Shasta Dam, Grand Coulee Dam, the Main Interior Building, and the Bureau of Reclamation's Supervisory Control and Data Acquisition computer system supporting dam operations as national critical infrastructures.

Results of Review

Based on its responses to the review guide, DOI has identified its critical assets, completed its initial vulnerability assessments, and resubmitted its CIPP to the Critical Infrastructure Assurance Office for review by an Expert Review Team (ERT). Although PDD-63 did not require DOI to notify the Office of Inspector General's (OIG) criminal investigations office of physical infrastructure attacks (see review step A19.e in Appendix 1), we consider it appropriate for DOI to notify the OIG when attacks on critical physical infrastructure have occurred. Also, DOI has taken action to incorporate the ERT's previously suggested improvements and to implement the two recommendations contained in our Phase I advisory letter. The two recommendations pertained to the establishment and implementation of a requirement to document the periodic threat review process and the resubmission of the CIPP to the ERT for approval.

The results of our review of DOI's critical physical infrastructure protection planning efforts under Phase 3 and the review steps that were developed by the PCIE working group are detailed in Appendix 1.

Recommendation

We recommend that DOI's Critical Infrastructure Assurance Officer (CIAO) establish a policy requiring that the OIG be notified when attacks on DOI's critical physical infrastructure assets occur.

Assistant Secretary for Policy, Management, and Budget Response and OIG Reply

In an August 14, 2001, response (Appendix 2) to the draft report, the Director, Office of Managing Risk and Public Safety (DOI's CIAO), concurred "with the spirit of the recommendation that the OIG be notified when attacks on DOI's critical physical infrastructure assets occur." The response further stated that the "policy can be effective immediately." The policy, however, was not prepared by the date we issued this final report. Based on the response, we consider the recommendation resolved and we are requesting additional information (Appendix 3).

In accordance with the Departmental Manual (360 DM 5.3), please provide us with your written response by January 31, 2002, regarding the target date for issuing a policy that requires OIG notification when attacks occur on DOI's critical physical infrastructure assets.

The legislation, as amended, creating the OIG, requires semiannual reporting to Congress on all audit reports issued, actions taken to implement audit recommendations, and identification of each significant recommendation on which corrective action has not been taken.

This advisory letter will be listed in our semiannual report to the Congress, as required by Section 5(a) of the Inspector General Act (5 U.S.C. app.3).

SCHEDULE OF REVIEW RESULTS

Review Step	Yes	No	N/A	Cause	Effect	Estimated Date of Resolution	Estimated Cost of Resolution	Estimate is in Agency CIP Budget	Recommendation
A.1 Has agency completed its Critical Infrastructure Protection Plan (CIPP)?	X								
A.2 If the agency does not plan to complete a CIPP, is it because it is not a Phase I/II agency subject to Presidential Decision Directive (PDD) 63 or among the agencies listed in the Critical Infrastructure Assurance Officer's (CIAO) Project Matrix?			X						
A.3 If the answer to question A.2 is yes, then identify the agency's physical assets that may be subject to PDD-63. Does agency management agree that any of the assets should be subject to PDD-63?			X						
A.4 For agencies that have prepared a CIPP, did the Critical Infrastructure Coordination Group sponsor the required "expert review process" for the CIPP? If an Expert Review Team (ERT) review was not performed, then determine the "cause" and continue with the remaining steps.	X								

Review Step	Yes	No	N/A	Cause	Effect	Estimated Date of Resolution	Estimated Cost of Resolution	Estimate is in Agency CIP Budget	Recommendation
A.5 If the Critical Infrastructure Coordination Group completed the expert review and found the CIPP deficient, has the agency taken adequate remedial action(s)?	X								
A.6 Does the CIPP require the appointment of a CIAO who will have overall responsibility for protecting the agency's critical infrastructure?	X								
A.7 Has the agency appointed a CIAO?	X								
A.8 Does the CIPP require the agency to identify its physical Mission Essential Infrastructure (MEI)?	X								
A.9 If the answer to question A.8 is yes, does the identification of assets include leased assets from the public or private sector?		X		DOI does not lease critical physical assets.					
A.10 Does the CIPP identify a milestone for identifying its physical MEI?	X								
A.11 Does the agency CIPP require an evaluation of new assets to determine whether they should be included in its MEI?	X								

Review Step	Yes	No	N/A	Cause	Effect	Estimated Date of Resolution	Estimated Cost of Resolution	Estimate is in Agency CIP Budget	Recommendation
A.12 Does the CIPP require the agency to perform vulnerability assessments of its physical MEI?	X								
A.13 Does the CIPP require periodic updates of the assessments?	X								
A.14 Does the CIPP identify milestones for completing the vulnerability assessments?	X								
A.15 Does the CIPP require risk mitigation relative to potential damage stemming from each vulnerability?	X								
A.16 Does the CIPP provide for periodic testing and re-evaluation of risk mitigation steps (policies, procedures, and controls) by agency management?	X								
A.17 Does the CIPP provide a milestone for taking steps to mitigate risks?	X								
A.18 Does the CIPP require establishment of an emergency management program?	X								

Review Step	Yes	No	N/A	Cause	Effect	Estimated Date of Resolution	Estimated Cost of Resolution	Estimate is in Agency CIP Budget	Recommendation
A.19.a If the answer to question A.18 is yes, does the CIPP specify that the emergency management program include the following: Incorporation of indications and warnings?	X								
A19.b Incident collection, reporting, and analysis?	X								
A19.c Response and continuity of operation plans?	X								
A19.d A system for responding to significant infrastructure attacks while the attacks are under way, with the goal of isolating and minimizing damage?	X								
A19.e Notification to OIG criminal investigators of infrastructure attacks?		X		DOI has existing linkages and close working relationships with Federal, state and local law enforcement agencies and intelligence sources.					Establish a policy requiring that the Office of Inspector General be notified when attacks occur on DOI's critical physical infrastructure assets.
A19.f Criteria for determining if an incident should be reported to the National Infrastructure Protection Center (NIPC) or Federal Computer Incident Response Capability (FedCIRC)?	X								

Review Step	Yes	No	N/A	Cause	Effect	Estimated Date of Resolution	Estimated Cost of Resolution	Estimate is in Agency CIP Budget	Recommendation
A19.g Procedures for reporting a computer security- or infrastructure-related incident to the NIPC?	**X**								
A.20 Does the CIPP require establishment of a system for quickly reconstituting minimum required capabilities following a successful infrastructure attack?	**X**								
A.21 Does the CIPP identify a milestone for establishing the emergency management program?	**X**								
A.22 Does the CIPP require a review of existing policies and procedures to determine whether the agency should revise them to reflect PDD-63 requirements?	**X**								
A.23 Does the CIPP identify a milestone for reviewing existing policies and procedures?	**X**								

Review Step	Yes	No	N/A	Cause	Effect	Estimated Date of Resolution	Estimated Cost of Resolution	Estimate is in Agency CIP Budget	Recommendation
A.24 Does the CIPP require the agency to incorporate its CIP functions into its strategic planning and performance measurement frameworks?		**X**		DOI's CIPP does not require the agency to include CIP functions in its strategic plan. This is because only certain assets of one (the Bureau of Reclamation) of the eight bureaus and the Main Interior Building are considered critical infrastructure. These assets constitute a small portion of DOI's overall infrastructure. DOI's strategic plan concentrates on DOI's major programmatic goals, such as protecting the environment and preserving natural and cultural resources.					
A.25 Does the CIPP identify a milestone for incorporating its critical infrastructure protection functions into its strategic planning and performance measurement frameworks?		**X**		See response to question A.24.					

Review Step	Yes	No	N/A	Cause	Effect	Estimated Date of Resolution	Estimated Cost of Resolution	Estimate is in Agency CIP Budget	Recommendation
A.26 Does the CIPP require agencies to identify resource and organizational requirements for implementing PDD-63?	X								
A.27 Does the CIPP identify a milestone for identifying resource and organizational requirements for implementing PDD-63?	X								
A.28 Does the CIPP require the agency to establish a program to ensure that it has the personnel and skills necessary to implement a sound infrastructure protection program?	X								
A.29 Does the CIPP identify a milestone for establishing a program that would ensure that the agency has the personnel and skills necessary to implement a sound infrastructure protection program?	X								
A.30 Does the CIPP require the agency to establish effective CIP coordination with other applicable entities (foreign, state, and local governments and industry)?	X								

Review Step	Yes	No	N/A	Cause	Effect	Estimated Date of Resolution	Estimated Cost of Resolution	Estimate is in Agency CIP Budget	Recommendation
A.31 Does the CIPP identify a milestone for establishing effective CIP coordination with other applicable entities (foreign, state, and local governments and industry)?	**X**								
A.32 Do the agency's plans for the continuous periodic review of its threat environment appear adequate, and is the agency complying with these plans?	**X**								
Identification of Critical Assets									
B.1 Has the agency identified its physical (non-cyber-based) MEI?	**X**								
B.1a Does the physical MEI include staff and management, such as security management and executives, needed to plan, organize, acquire, deliver, support, and monitor mission-related services, information systems, and facilities)?	**X**								
B.1.b Does the physical MEI include facilities (all facilities required to support the core processes, including these support information technology resources)?	**X**								

Review Step	Yes	No	N/A	Cause	Effect	Estimated Date of Resolution	Estimated Cost of Resolution	Estimate is in Agency CIP Budget	Recommendation
B.2.a Evaluate the adequacy of the agency's' efforts to identify MEI and MEI interdependencies with applicable Federal agencies, state and local government activities, and/or industry. Has the agency identified critical, physical assets consistent with the criteria in footnote 1 of the Phase III review guide?	**X**								
B.2.b Has the agency identified interdependencies for its critical physical assets?	**X**								
B.2.c Did the agency use the CIAO infrastructure asset evaluation survey to identify its MEI assets?		**X**		The critical physical infrastructure was identified and CIPP was prepared in June 1999, which was before the effective date of the criteria (January 2000).					

Review Step	Yes	No	N/A	Cause	Effect	Estimated Date of Resolution	Estimated Cost of Resolution	Estimate is in Agency CIP Budget	Recommendation
B.2.d Did the asset identification process include a determination of the estimated replacement cost, planned life cycle, and potential impact to the agency if the asset is rendered unusable?		X		The asset identification process included a determination of the potential impact of assets that are rendered unusable. DOI officials said, however, that they did not consider it necessary to estimate the replacement cost and planned life cycle of assets that were rendered unusable.					
B.2.e Has the agency established milestones for identifying and reviewing its MEI?	X								
B.2.f Is the agency meeting its milestones?	X								
Vulnerability Assessments									
C.1 Has the agency performed and documented an initial vulnerability assessment and developed remediation plans for its MEI?	X								

Review Step	Yes	No	N/A	Cause	Effect	Estimated Date of Resolution	Estimated Cost of Resolution	Estimate is in Agency CIP Budget	Recommendation
C.2 Did the vulnerability assessments address the threat type and magnitude of the threat, the source of the threats, existing protection measures, the probability of occurrence, damage that could result from a successful attack, and the likelihood of success if such an attack occurred?	**X**								
C.3 Did the remediation plans address the vulnerabilities found during the assessment?	**X**								
C.4 Has the agency determined the level of protection currently in place for its MEI?	**X**								
C.5 Has the agency identified the actions that must be taken before it can achieve a reasonable level of protection for its MEI?	**X**								
C.6 If your answer to number 5 is yes, then has the agency developed a related implementation plan and mechanism to monitor such implementation?	**X**								

Review Step	Yes	No	N/A	Cause	Effect	Estimated Date of Resolution	Estimated Cost of Resolution	Estimate is in Agency CIP Budget	Recommendation
C.7 Has the agency delegated responsibility for vulnerability assessments to the agency CIO or CIAO?	X								
C.8 Has the agency adopted a multi-year funding plan that addresses the identified threats?	X								
C.9 Has the agency reflected the cost of implementing a multi-year vulnerability remediation plan in its budget submissions to OMB?	X								
C.10 Did the vulnerability assessments query national threat guidance for international, domestic, and state-sponsored terrorism/information warfare (e.g., from the DoD, FBI, NSA, and other Federal and state agencies)?	X								
C.11 Has the agency prioritized the threats according to their relative importance?	X								

Review Step	Yes	No	N/A	Cause	Effect	Estimated Date of Resolution	Estimated Cost of Resolution	Estimate is in Agency CIP Budget	Recommendation
C.12 Has the agency assessed the vulnerability of its MEI to failures that could result from interdependencies with applicable Federal agency and state and local government activities and private sector providers of telecommunications, electrical power, and other infrastructure services?	X								
C.13 Do the processes used to identify and reflect new threats to the agency's MEI appear adequate?	X								
C.14 Do the results of the vulnerability assessments necessitate revisions to agency policies that govern the management and protection of agency MEI?	X								
C.15 Did the results of the ERT coincide with answers derived from questions A.1 through C.14?	X								

United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, D.C. 20240

August 14, 2001

Memorandum

To: Roger LaRouche
Assistant Inspector General for Audits

From: L. Michael Kaas
Director, Office of Managing Risk and Public Safety

Subject: Draft Advisory Letter on Critical Infrastructure Assurance Program, Department of the Interior (Assignment No. H-IN-OSS-003-01 R)

We have reviewed the Draft Advisory Letter dated July 2, 2001, dealing with the Phase 3 review of critical physical infrastructure protection planning. We concur with the spirit of the recommendation that the Office of the Inspector General (OIG) be notified when attacks on DOI's critical physical infrastructure assets occur. To be more operationally sound, the recommendation should be rephrased. The notification should be made by the Director of the Office of Managing Risk and Public Safety (MRPS) who serves as the Department's Critical Infrastructure Assurance Officer (CIAO). This policy can be effective immediately.

cc: Chief Information Officer (CIO), Office of Information Resources Management

STATUS OF ADVISORY LETTER RECOMMENDATION

Recommendation	Status	Action Required
1	Management concurs; additional information needed.	Provide a target date for issuance of a policy on notifying OIG when attacks occur on DOI's critical physical infrastructure assets

Mission

The mission of the Office of Inspector General (OIG) is to promote excellence in the programs, operations, and management of the Department of the Interior (DOI). We accomplish our mission in part by objectively and independently assessing major issues and risks that directly impact, or could impact, the DOI's ability to carry out its programs and operations and by timely advising the Secretary, bureau officials, and the Congress of actions that should be taken to correct any problems or deficiencies. In that respect, the value of our services is linked to identifying and focusing on the most important issues facing DOI.

How to Report Fraud, Waste, and Abuse

Fraud, waste, and abuse in Government are the concern of everyone - Office of Inspector General staff, Departmental employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and abuse related to Departmental or insular area programs and operations. You can report allegations to us by:

Mail:

U.S. Department of the Interior
Office of Inspector General
Mail Stop 5341-MIB
1849 C Street, NW
Washington, DC 20240

Phone:

24-Hour Toll Free	**800-424-5081**
Washington Metro Area	**202-208-5300**
Hearing Impaired	**202-208-2420**
Fax	**202-208-6023**
Caribbean Region	**703-487-8058**
Northern Pacific Region	**671-647-6060**

Internet: **www.oig.doi.gov/hotline_form.html**