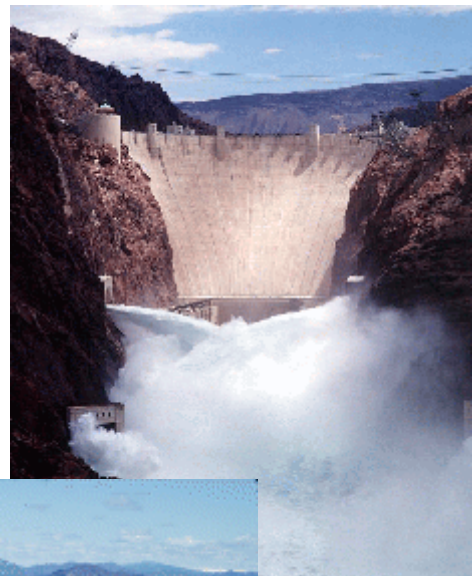


**U.S. Department of the Interior  
Office of Inspector General**

## **Advisory Letter**

### **Critical Infrastructure Assurance Program, Department of the Interior**



**Report No. 00-I-704  
September 2000**



# United States Department of the Interior

E-IN-OSS-010-00-R

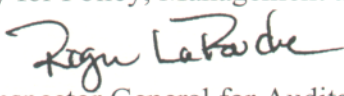
OFFICE OF INSPECTOR GENERAL  
Washington, D.C. 20240

September 29, 2000

## Advisory Letter

### Memorandum

To: Assistant Secretary for Policy, Management and Budget

From: Roger La Rouché   
Acting Assistant Inspector General for Audits

Subject: Advisory Letter on Critical Infrastructure Assurance Program,  
Department of the Interior (No. 00-I-704)

As requested by the President's Council on Integrity and Efficiency (PCIE), we reviewed the Department of the Interior's Critical Infrastructure Assurance Program. This review is being conducted as part of a Governmentwide evaluation of Federal agency implementation of Presidential Decision Directive 63 (PDD-63), which called for a national effort to ensure the security of the Nation's critical physical and cyber-based infrastructures.<sup>1</sup> This letter presents the results of our review of Departmental actions under Phase 1 (cyber-based planning) of the four-phase PCIE review. Our objective was to determine whether Departmental plans, asset identification efforts, and initial vulnerability assessments were adequate to protect critical Departmental infrastructures.

## Results of Review

---

We found that the Department has made significant progress toward implementing PDD-63 (see the Schedule of Review Results in the Appendix 1). However, we did not make a determination regarding cyber vulnerability assessments because the assessments to identify vulnerabilities and recommend corrective actions are under way and are scheduled for completion in the fall of 2000. We found that the Department had adequately identified the critical assets and submitted its Critical Infrastructure Protection Plan (CIPP) to the National Critical Assurance Office for review by an Expert Review

---

<sup>1</sup>Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government, including telecommunications, energy, banking and finance, transportation, water systems, and emergency services, both governmental and private.

completion in the fall of 2000. We found that the Department had adequately identified the critical assets and submitted its Critical Infrastructure Protection Plan (CIPP) to the National Critical Assurance Office for review by an Expert Review Team (ERT). The Department has taken or plans to take the actions necessary to incorporate the ERT's suggested improvements.

We also found, that the Department had not documented the results of the periodic reviews regarding its threat environment.<sup>2</sup> The Departmental Manual (375 DM 19.8) states:

Each bureau will conduct periodic reviews of its Information Technology (IT) security program to determine its effectiveness and to re-certify the adequacy of the installed security safeguards. These reviews may use existing reports, such as those prepared for risk analyses, IT certifications, Privacy Act inspections, Departmental Management Control Evaluations, and Inspector General audits. The results of these reviews should serve as a basis for the annual bureau IT security Plan.

Departmental IT officials told us that these reviews were performed for each bureau but were not documented. We believe that the review process should have included written notifications to bureaus concerning the review, analysis, assessments, implementation of corrective actions, and results of the review. In that regard, without adequate documentation of the review process, there was no accountability for the actions taken.

## **Recommendations**

---

We recommend that the Department's Chief Information Officer (CIO):

1. Ensure that the Department establishes and implements a requirement to document the periodic threat review process that includes written notifications to bureaus concerning the review, analysis, assessments, and implementation of corrective actions.

2. Ensure that the CIPP is resubmitted to the ERT for approval.

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

---

---

<sup>2</sup>Threats can be external (from outside the organization) or internal (from employees or contractors). Threats also are natural (earthquakes or hurricanes), accidental (equipment failure or operator errors), or intentional (terrorists, hackers, or malicious employees).

In the September 27, 2000 response (Appendix 2) to the draft report from the Assistant Secretary for Policy, Management and Budget (AS/PMB), the AS/PMB concurred with the recommendations. The AS/PMB further stated that the CIO will, by December 15, 2000, ensure that the Department establishes and implements a requirement to document the periodic threat review process that includes written notifications to bureaus concerning the review, analysis, assessments, and implementation of corrective actions (Recommendation 1). It further stated that by December 15, 2000, the requirement to document the periodic threat review process will be included in the Department's Critical Infrastructure Protection Plan and submitted to the National Critical Assurance Office for review by the ERT (Recommendation 2).

Based on the response, we consider both recommendations resolved but not implemented (Appendix 3). Accordingly, the unimplemented recommendation will be referred to your Office of Financial Management for tracking of implementation.

## **Scope of Review**

---

Our review was conducted as part of a Governmentwide four-phase PCIE review on implementation of PDD-63. To accomplish our review, we conducted interviews with the Critical Infrastructure Assurance Officer and his staff, the CIO, and other IT officials to obtain information concerning the critical infrastructures and planning processes used by the Department. The four phases will review the adequacy of:

- Agency planning and assessment activities for protecting critical physical and cyber-based infrastructures (Phase 1).
- 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).

The results of our review of the Departmental cyber-based planning efforts under Phase 1 and the review steps that were developed by the PCIE working group are detailed in Appendix 1. The results of the review will also be sent to the PCIE working group for inclusion in a governmentwide report concerning the security of Federal critical infrastructures.

## **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, which was 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 Federal Government to protect the national security and ensure general public health and safety; of the state and local governments to maintain order and deliver minimum essential public services; and of the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial, and transportation services. PDD-63 further directs the Federal Government to eliminate any significant vulnerability to both physical and cyber attacks on its critical infrastructures by May 22, 2003.

The Department's CIPP identified Hoover Dam, Shasta Dam, Grand Coulee Dam, and the Main Interior Building and the Bureau of Reclamation's Supervisory Control and Data Acquisition computer system supporting dam operations as national critical infrastructures.

Since this letter's recommendations are considered resolved, no further response to the Office of Inspector General is required ( see Appendix 3).

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

## SCHEDULE OF REVIEW RESULTS

Review Step (a)(b)	Yes (c)	No (d)	N/A (e)	Cause If "No" Answer in Column (d) (f)	Effect (g)	Estimated Date of Resolution (h)	Estimated Cost of Resolution (i)	Estimate is in Agency CIP Budget (j)	Recommendation (k)
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?			X						
A.3 Identify agency's cyber-based 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 the remaining steps.	X								
A.5 If the Critical Infrastructure Coordination Group completed the expert review and found the CIPP to be deficient, has the agency taken adequate remedial action(s)?		X		The Department incorporated many of the Expert Review Team's suggested improvements and has made further revisions during our audit.	N/A	Jul-00	N/A	N/A	Ensure that the CIPP is resubmitted to the ERT for approval.
A.6 Did the CIPP require the appointment of a Chief Infrastructure Assurance Officer (CIAO), who will have overall responsibility for protecting the agency's critical infrastructure?	X								
A.7 Has the agency appointed a CIAO?	X								

Review Step (a)(b)	Yes (c)	No (d)	N/A (e)	Cause If "No" Answer in Column (d) (f)	Effect (g)	Estimated Date of Resolution (h)	Estimated Cost of Resolution (i)	Estimate is in Agency CIP Budget (j)	Recommendation (k)
A.8 Does the CIPP require the agency to identify its cyber-based Mission Essential Infrastructure (MEI)?	X								
A.9 Does the CIPP identify a milestone for identifying its cyber-based MEI?		X		The identification of cyber-based MEI was completed prior to developing the CIPP.	N/A	N/A	N/A	N/A	N/A
A.10 Does the agency CIPP require an evaluation of new assets to determine whether they should be included in its MEI?	X								
A.11 Does the CIPP require the agency to perform vulnerability assessments of its cyber-based MEI?	X								
A.12 Does the CIPP require periodic updates of the assessments?	X								
A.13 Does the CIPP identify milestones for completing the vulnerability assessments?	X								
A.14 Does the CIPP require risk mitigation relative to potential damage stemming from each vulnerability?	X								
A.15 Does the CIPP provide for periodic testing and reevaluation of risk mitigation steps (policies, procedures, and controls) by agency management?	X								
A.16 Does the CIPP provide a milestone for taking steps to mitigate risks?	X								
A.17 Does the CIPP require establishment of an emergency management program?	X								

Review Step (a)(b)	Yes (c)	No (d)	N/A (e)	Cause If "No" Answer in Column (d) (f)	Effect (g)	Estimated Date of Resolution (h)	Estimated Cost of Resolution (i)	Estimate is in Agency CIP Budget (j)	Recommendation (k)
A.18. If the answer to A.17 is yes, does the CIPP specify that the emergency management program includes: a) Incorporation of indications and warnings?	X								
b) Incident collection, reporting, and analysis?	X								
c) Response and continuity of operation plans?	X								
d) A system for responding to significant infrastructure attacks while the attacks are under way, with the goal of isolating and minimizing damage?	X								
e) Notification to OIG criminal investigators of infrastructure attacks?		X		Although the CIPP did not include a requirement to notify the OIG, the Departmental Manual (375 DM 19.9, B(2)) requires the notification.	N/A	N/A	N/A	N/A	N/A
A.19 Does the CIPP require establishment of a system for quickly reconstituting minimum required capabilities following a successful infrastructure attack?		X		Although the CIPP did not include a requirement to establish a system for quickly reconstituting minimum required capabilities following a successful infrastructure attack, it was required by the Departmental Manual (375 DM 19.4, H and K) to do so.	N/A	N/A	N/A	N/A	N/A
A.20 Does the CIPP identify a milestone for establishing the emergency management program?	X								



Review Step (a)(b)	Yes (c)	No (d)	N/A (e)	Cause If "No" Answer in Column (d) (f)	Effect (g)	Estimated Date of Resolution (h)	Estimated Cost of Resolution (i)	Estimate is in Agency CIP Budget (j)	Recommendation (k)
A.21 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		Departmental officials implemented a requirement for a review that ensures that PDD 63 requirements are followed. In addition, this review is required by the Departmental Manual (375 DM 19.4, C).	N/A	N/A	N/A	N/A	N/A
A.22 Does the CIPP identify a milestone for reviewing existing policies and procedures?		X		During our review, Department officials implemented a requirement for annual milestones.	N/A	Jul-00	N/A	N/A	N/A
A.23. Does the CIPP require the agency to ensure that security planning procedures are being incorporated into the basic design of new programs that include critical infrastructures, including provisions for:  a) Risk management and assessments?		X		Although the CIPP did not include a requirement to ensure that security planning procedures were being incorporated into the basic design of new programs that include critical infrastructures, this is required by the Departmental Manual (375 DM 19.4,B).	N/A	N/A	N/A	N/A	N/A
b) Security plans for IT systems?	X								
c) Security for command, control, and communications?	X								
d) Identification of classified or sensitive information?	X								
e) Awareness and training measures to be taken for each program?	X								

Review Step (a)(b)	Yes (c)	No (d)	N/A (e)	Cause If "No" Answer in Column (d) (f)	Effect (g)	Estimated Date of Resolution (h)	Estimated Cost of Resolution (i)	Estimate is in Agency CIP Budget (j)	Recommendation (k)
A.24 Does the CIPP identify a milestone for establishing procedures to ensure that the agency incorporates security planning into the basic design of new programs?		X		Although the CIPP did not identify a milestone for establishing procedures to ensure that the agency incorporates security planning into the basic design of new programs, it is required by the Departmental Manual (375 DM 19.4, B).	N/A	N/A	N/A	N/A	N/A
A.25 Does the CIPP require the agency to incorporate its CIP functions into its strategic planning and performance measurement frameworks?		X		The Department's CIPP does not require the agency to include Critical Infrastructure Planning functions in its strategic plan. This is because only one (BOR) of the eight bureaus is directly involved with Critical Infrastructure and then only in a small part of its overall program. The strategic plan concentrates on the major Departmental goals for protecting the environment, preserving natural and cultural resources, providing recreation, conducting scientific studies, and meeting responsibilities to American Indians.	N/A	N/A	N/A	N/A	N/A
A.26 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 A.25.	N/A	N/A	N/A	N/A	N/A

Review Step (a)(b)	Yes (c)	No (d)	N/A (e)	Cause If "No" Answer in Column (d) (f)	Effect (g)	Estimated Date of Resolution (h)	Estimated Cost of Resolution (i)	Estimate is in Agency CIP Budget (j)	Recommendation (k)
A.27 Does the CIPP require agencies to identify resource and organizational requirements for implementing PDD 63?	X								
A.28 Does the CIPP identify a milestone for identifying resource and organizational requirements for implementing PDD 63?		X		The milestone will be established pending the completion of the vulnerability assessment work that is in progress.	N/A	Sep-00	\$270,000	N/A	N/A
A.29 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.30 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.31 Does the CIPP require the agency to establish effective CIP coordination with other applicable entities (foreign, state, and local governments and industry)?	X								
A.32 Does the CIPP identify a milestone for establishing effective CIP coordination with other applicable entities (foreign, state, and local governments and industry)?	X								
A.33 Are the agency's plans for the continuous / periodic review of its threat environment: a) Adequate?	X								

Review Step (a)(b)	Yes (c)	No (d)	N/A (e)	Cause If "No" Answer in Column (d) (f)	Effect (g)	Estimated Date of Resolution (h)	Estimated Cost of Resolution (i)	Estimate is in Agency CIP Budget (j)	Recommendation (k)
b) Being implemented by the agency?		X		The Departmental Manual (375 DM 19.8) requires the Office of Information Resources Management to conduct periodic reviews. Departmental IT officials told us that these reviews were performed for each bureau but were not documented. We believe that the review process should have included written notifications to bureaus concerning the review, analysis, assessments, and implementation of corrective actions and results of the review.	We believe that without adequate documentation of the review process, there is a lack of accountability for the actions taken.				Ensure that the Department establishes and implements a requirement to document the periodic threat review process that includes written notifications to bureaus concerning the review, analysis, assessments, and implementation of corrective actions.
B.1. Has the agency identified the following cyber-based MEI:  a) People? (Staff, management, security, and executives necessary to plan, organize, acquire, deliver, support, and monitor mission-related services, information systems, and facilities, including the groups and individuals external to the organization involved in the fulfillment of the organization's mission.)	X								
b) Technology? (All hardware and software, connectivity, countermeasures, and/or safeguards that are utilized in support of the core process.)	X								
c) Applications? (All application systems, internal and external, utilized in support of the core process.)	X								

Review Step (a)(b)	Yes (c)	No (d)	N/A (e)	Cause If "No" Answer in Column (d) (f)	Effect (g)	Estimated Date of Resolution (h)	Estimated Cost of Resolution (i)	Estimate is in Agency CIP Budget (j)	Recommendation (k)
d) Data? (All data, electronic / hard copy, and information required to support the core process. These data include numbers, characters, images, or other methods of recording in a form that can be assessed by a human or input into a computer, stored and processed there, or transmitted on some digital/communications channel.)	X								
e) Facilities? (All facilities required to support the core processes, including the resources to house and support information technology resources, and the other resource elements defined above in question B.1.)	X								
B.2a Were the criteria used to identify DOI's MEI consistent with the criteria used by the CIAO to identify agency MEI? (See page 1, footnote 1, for CIAO definition of agency MEI.)	X								
B.2b Did the agency use the CIAO infrastructure asset evaluation survey to identify its MEI assets?		X		The CIPP was prepared in June 1999, which was before the effective date of the criteria (January 2000).	N/A	N/A	N/A	N/A	N/A
B.3 Evaluate the adequacy of the agency's efforts to identify MEI and MEI interdependencies with applicable Federal agencies, state and local government activities, and industry:  a) Has the agency identified assets consistent with the MEI as defined in question B.2?	X								
b) Did the agency use the results of its Year 2000 (Y2K) work in identifying the MEI?	X								

Review Step (a)(b)	Yes (c)	No (d)	N/A (e)	Cause If "No" Answer in Column (d) (f)	Effect (g)	Estimated Date of Resolution (h)	Estimated Cost of Resolution (i)	Estimate is in Agency CIP Budget (j)	Recommendation (k)
c) Did the asset identification process include a determination of its estimated replacement costs, planned life cycle, and potential impact to the agency if the asset is rendered unusable?	X								
d) Has the agency established milestones for identifying and reviewing its MEI?	X								
e) Is the agency meeting its milestones?	X								
C.1 Has the agency performed and documented an initial vulnerability assessment and developed redemption plans for its MEI?		X		Pending the completion of the vulnerability assessment work that is in progress.	N/A	Sep-00	See A. 28	N/A	N/A
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	Pending the completion of the vulnerability assessment work that is in progress.	N/A	N/A	N/A	N/A	N/A
C.3 Did the redemption plans address the vulnerabilities found during the assessment?			X	Pending the completion of the vulnerability assessment work that is in progress.	N/A	Oct-00	N/A	N/A	N/A
C.4 Has the agency determined the level of protection currently in place for its MEI?			X	Pending the completion of the vulnerability assessment work that is in progress.	N/A	Aug-00	N/A	N/A	N/A
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	Pending the completion of the vulnerability assessment work that is in progress.	N/A	Aug-00	N/A	N/A	N/A
C.6 If the answer to C. 5 is yes, has the agency developed a related implementation plan and mechanism to monitor such implementation?			X	Pending the completion of the vulnerability assessment work that is in progress.	N/A	Oct-00	N/A	N/A	N/A

Review Step (a)(b)	Yes (c)	No (d)	N/A (e)	Cause If "No" Answer in Column (d) (f)	Effect (g)	Estimated Date of Resolution (h)	Estimated Cost of Resolution (i)	Estimate is in Agency CIP Budget (j)	Recommendation (k)
C.7 Has the agency delegated responsibility for vulnerability assessments to the agency CIO?	X								
C.8 Has the agency adopted a multi-year funding plan that addresses the identified threats?		X		BOR has identified estimated funding needs for its security-related issues. These will need further refinement once results of Sandia National Laboratory (SNL) recommendations have been evaluated.	N/A	Oct-00	N/A	N/A	N/A
C.9 Has the agency reflected the cost of implementing a multi-year vulnerability redemption plan in its FY 2001 budget submission to the Office of Management and Budget?		X		Estimated adjustments to the FY 2001 budget have been made. Determination of more precise requirements will result from the evaluation of the SNL recommendations.	N/A	Sep-00	N/A	N/A	N/A
C.10 Did the vulnerability assessments query national threat guidance for international, domestic, and state-sponsored terrorism/information warfare (e.g., from the Department of Defense, FBI, NSA, and other Federal and state agencies)?			X	Pending the completion of the vulnerability assessment work that is in progress.	N/A	Sep-00	N/A	N/A	N/A
C.11 Has the agency prioritized the threats according to their relative importance?			X	Pending the completion of the vulnerability assessment work that is in progress.	N/A	Sep-00	N/A	N/A	N/A
C.12 Has the agency assessed the vulnerability of its MEI to possible failures that could result from interdependencies with applicable Federal agencies, state and local government activities, and private sector providers of telecommunications, electrical power, and other infrastructure services?	X								

Review Step (a)(b)	Yes (c)	No (d)	N/A (e)	Cause If "No" Answer in Column (d) (f)	Effect (g)	Estimated Date of Resolution (h)	Estimated Cost of Resolution (i)	Estimate is in Agency CIP Budget (j)	Recommendation (k)
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	The preparation of security policies and procedures are currently ongoing, along with the vulnerability assessment.	N/A	Sep-00	N/A	N/A	N/A
C.15 Did the results of the ERT coincide with answers derived from questions A.1 through C.14?	X								



**STATUS OF EVALUATION REPORT RECOMMENDATIONS**

Recommendation Reference	Status	Action Required
1 and 2	Resolved; not implemented	No further response to response to the Office of Inspector General is required. The recommendations will be referred to your Office of Financial Management for tracking of implementation.

**ILLEGAL OR WASTEFUL ACTIVITIES  
SHOULD BE REPORTED TO  
THE OFFICE OF INSPECTOR GENERAL**

---

**Internet Complaint Form Address**

**[http://www.oig.doi.gov/hotline\\_form.html](http://www.oig.doi.gov/hotline_form.html)**

**Within the Continental United States**

U.S. Department of the Interior  
Office of Inspector General  
1849 C Street, N.W.  
Mail Stop 5341 - MIB  
Washington, D.C. 20240-0001

Our 24-hour  
Telephone HOTLINE  
1-800-424-5081 or  
(202) 208-5300

TDD for hearing impaired  
(202) 208-2420

**Outside the Continental United States**

***Caribbean Region***

U.S. Department of the Interior  
Office of Inspector General  
Eastern Division - Investigations  
4040 Fairfax Drive  
Suite 303  
Arlington, Virginia 22203

(703) 235-9221

***Pacific Region***

U.S. Department of the Interior  
Office of Inspector General  
Guam Field Pacific Office  
415 Chalan San Antonio  
Baltej Pavilion, Suite 306  
Agana, Guam 96911

(671) 647-6060

---

# HOTLINE

U.S. Department of the Interior  
Office of Inspector General  
1849 C Street, NW  
Mail Stop 5341- MIB  
Washington, D.C. 20240-0001

Toll Free Number  
1-800-424-5081

Commercial Numbers  
(202) 208-5300  
TDD (202) 208-2420

