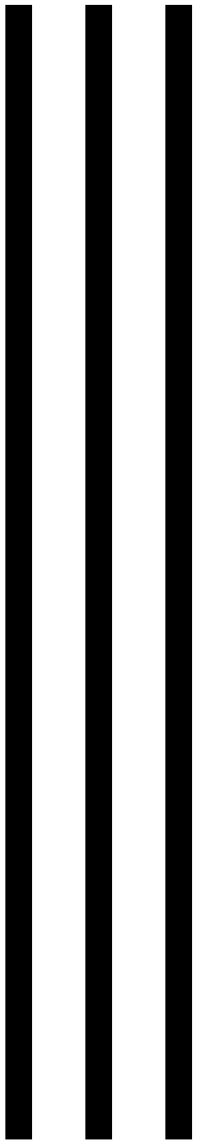

U.S. Department of Agriculture
Office of Inspector General
Audit Report

Office of Procurement and Property Management
Physical Critical Infrastructure Protection Program

Report No.
50099-4-HQ
October 2001

UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington, D.C. 20250

DATE: October 16, 2001

REPLY TO
ATTN OF: 50099-4-HQ

SUBJECT: PCIE/ECIE Physical Critical Infrastructure Protection Program

TO: Russ Ashworth
Director
Office of Procurement and Property Management

The President's Council on Integrity and Efficiency (PCIE) initiated a multi-phased review of the Nation's critical infrastructure assurance as required by Presidential Decision Directive (PDD) 63, "Policy on Critical Infrastructure Protection," issued May 22, 1998. On July 18, 2000, we reported to the Chief Information Officer (Audit Report No. 50099-28-FM) on Phase I of the PCIE review related to cyber-based critical infrastructures within the U.S. Department of Agriculture (USDA). This memorandum report presents the results of our audit performed as part of Phase III of the PCIE review on physical critical infrastructures. To carry out our audit, we reviewed the adequacy of the Department's plans and actions taken to protect physical assets and facilities in accordance with PDD 63.

We concluded that USDA's Office of Procurement and Property Management (OPPM) had appropriately planned for protection and security of physical critical infrastructure in accordance with PDD 63. However, not all minimum essential infrastructure (MEI) had been identified because USDA-owned facilities were not included in the database used by USDA to identify critical facilities. In addition, because of a lack of resources, assessments by USDA of identified critical facilities cannot be performed timely.

In its response to the official draft report, dated September 27, 2001, OPPM generally agreed with our findings and recommendations and agreed to implement corrective action. The entire response is included as attachment A to this report.

BACKGROUND

The Clinton Administration's Policy on Critical Infrastructure Protection: PDD 63, May 1998, calls for a national effort to assure the security of the Nation's critical infrastructures–also known as MEI. Critical infrastructures are defined as those physical and cyber-based systems essential

to the minimum operations of the economy and Government. Critical infrastructures include, but are not limited to, telecommunications, banking and finance, energy, transportation, and essential Government services.

The President intended that the United States take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our Nation's critical infrastructures especially our cyber systems. By May 22, 2003, the United States shall have achieved and shall maintain the ability to protect its critical infrastructures from intentional acts that would significantly diminish the abilities of:

- the Federal Government to perform essential national security missions and to ensure the general public health and safety;
- State and local governments to maintain order and to 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.

Also, as part of PDD 63, the President authorized the Federal Bureau of Investigation (FBI) to expand its current organization to a full scale National Infrastructure Protection Center (NIPC). The Center is to serve as a focal point in the Federal Government for gathering information on threats as well as facilitating and coordinating the Federal Government's response to incidents impacting key infrastructures. Further, the Center is to issue attack warnings to private sector and government entities as well as alerts to increases in threat conditions.

Within USDA, the Office of the Chief Information Officer (OCIO) is responsible for security of cyber-based systems. OCIO developed a Critical Infrastructure Assurance Plan to address the requirements of PDD 63 related to cyber-based critical infrastructures. We reviewed this plan during the audit work we performed for Phase I of the critical infrastructure review. Physical critical infrastructures and security of related assets and facilities is the responsibility of the Assistant Secretary for Administration (ASA) and specifically of OPPM.

OPPM has developed a plan to assess physical critical infrastructure including identification and assessment of MEI. At the time of our review, OPPM had identified 121 critical facilities within USDA and performed assessments on 4 of these facilities in the Kansas City, Missouri, area. OPPM has also drafted policies and procedures for security of USDA facilities. These policies should be implemented sometime in fiscal year 2002.

OBJECTIVES

Our overall objective was to review the adequacy of the Department's planning and assessment activities for protecting its critical, physical (non-cyber-based) infrastructures. Specifically, we reviewed the adequacy of the Department's plans, asset identification efforts, and initial vulnerability assessments.

SCOPE AND METHODOLOGY

The scope of our work was from May 22, 1998 (when PDD 63 was issued), to the present regarding the Department's planning and assessment activities for protecting its critical, physical (non-cyber-based) infrastructures. We obtained and reviewed the Department's plans to identify and assess its physical MEI. We also interviewed personnel from OCIO and OPPM and reviewed draft security policies prepared by OPPM.

We conducted our audit during January 2001 and May through June 2001.[1] The audit was conducted in accordance with Government Auditing Standards.

FINDINGS

Overall, we concluded that USDA has made appropriate plans to assure the security of its physical critical infrastructures including identifying and assessing physical MEI. However, although the plans appear to be appropriate, not all physical MEI had been identified and because of a lack of resources, vulnerability assessments cannot be timely performed for all critical facilities. We also noted that draft security policies did not include a provision to report any infrastructure-related incidents to the NIPC. Details follow.

1. PDD 63 called for a national effort to assure the security of the Nation's critical infrastructures–also known as MEI–by identifying and assessing the vulnerabilities of these critical infrastructures to attack. OPPM advised us that it had identified 121 critical mission essential facilities (or MEI) within USDA based on a database maintained by the Federal Protective Service (FPS). According to OPPM, this listing identified the most critical and essential USDA facilities including labs, the National Finance Center, and structures housing computer systems. However, our review of the listing of 121 facilities disclosed that some critical USDA facilities, including labs at Plum Island, New York, and Ames, Iowa, were not included on the list. After discussing this with OPPM, it was discovered that the FPS database did not include USDA-owned facilities. A new staff member at OPPM had assumed these facilities were included by FPS. An OPPM official advised us that because the owned and commercially leased real property database is currently being migrated to a new system, agencies would have to be contacted directly to identify critical USDA-owned facilities, which will be a very time-consuming process. OPPM has started gathering this information.

2. As discussed previously, PDD 63 requires agencies to assess the vulnerabilities of its critical infrastructures. OPPM plans to assess each of USDA's critical facilities during site visits to each facility. As of the date of our audit, OPPM had only performed site visits and assessments of four facilities in the Kansas City, Missouri, area. OPPM plans to visit and assess all critical facilities at a rate of 10 facilities per year (budget allowing). At this rate, all 121 identified critical facilities will not be assessed until 2013–well beyond the 2003 date indicated by PDD 63 as when the Nation will be able to maintain the ability to protect its

[1] Audit work was suspended from January through May 2001 due to other priorities.

critical infrastructure. According to an OPPM official, additional funding is needed to carry out this program. Currently, only one person within OPPM has the responsibility to visit and perform the assessments. Furthermore, as stated above, USDA-owned critical facilities have not been identified. This coupled with a lack of resources could delay performance of necessary vulnerability assessments even further.

3. PDD 63 authorized the FBI to expand its organization to a full scale NIPC. NIPC includes FBI and other investigators experienced in infrastructure protection. Its mission includes providing timely warnings of intentional threats to critical infrastructures and response to these threats. All executive departments within the Government are to share information about threats and warnings of attacks on critical Government facilities with NIPC. We noted that draft security policies prepared by OPPM do not include provisions or criteria for determining if an incident should be reported to NIPC. An OPPM official informed us that reporting incidents to NIPC had not been considered when the policies were drafted, but OPPM will include this provision as part of the security policies that should be in place in fiscal year 2002.

With assets of $124 billion and an extensive range of critical missions related to public health, rural development, and food safety, it is essential that USDA's critical facilities and assets be identified and assessed for threats of attack. In addition, the Federal Critical Infrastructure Assurance Office designated USDA as one of the 14 agencies having systems, if sabotaged, could cripple the Nation's economy and security. Based on the issues we identified, prompt actions are necessary to ensure the protection of USDA's physical critical infrastructures.

RECOMMENDATIONS

1. Work with USDA agencies to generate a listing of USDA-owned and commercially leased facilities and use this listing to identify mission essential facilities (or MEI) owned and leased by USDA.

2. Pursue additional funding to ensure adequate resources and staff with the necessary skills are available to perform needed vulnerability assessments of critical USDA facilities and to carry out other necessary provisions of PDD 63.

3. Include provisions in the security policies being developed for criteria to determine when a security or infrastructure-related incident should be reported to NIPC and procedures for reporting such incidents.

AGENCY RESPONSE

In its response, dated September 27, 2001, OPPM agreed to take corrective actions. It stated that key USDA personnel have been contacted to identify all USDA-owned and leased facilities and the list of facilities identified as MEI and the schedule to visit the sites will be completed by December 2001. OPPM will also pursue funding to ensure adequate resources are available to perform needed vulnerability assessments and to carry out the provisions of PDD 63.

Furthermore, OPPM will develop policies and procedures to conduct security assessments of all USDA facilities and include provisions for determining when a security incident should be reported to NIPC. Draft policies will be completed by October 31, 2001. (See attachment A for the full text of OPPM's response.)

OIG POSITION

We accept OPPM's management decision on all recommendations.

Departmental Regulation 1720-1 requires that final action be completed within 1 year of the date of management decision. Please follow your internal agency procedures in forwarding final action correspondence to the Office of the Chief Financial Officer. We appreciate the courtesies and cooperation extended to our staff during this review.

/S/

RICHARD D. LONG
Assistant Inspector General
for Audit

ATTACHMENT A – OPPM RESPONSE

United States Department of Agriculture

Office of the Assistant Secretary for Administration

Office of Procurement and Property Management

300 7th Street Southwest
Room 302
Reporters Building

Washington, DC
20024-9300

TO: Richard D. Long
Assistant Inspector General for Audit
Office of Inspector General

FROM: W. R. Ashworth
Director

SEP 27 2001

SUBJECT: PCIE/ECIE Physical Critical Infrastructure Protection Program (500099-4-HQ)

In response to your official draft report on the PCIE/ECIE Physical Critical Infrastructure Protection Program, dated July 20, 2001, below are the corrective actions to be taken to address the audit findings, conclusions, and recommendations. It must be said that due to limited resources, corrective action completions may not be accomplished by the date established in PDD 63. However, all corrective actions will have completion phases as a part of their overall scheduling, and all reasonable efforts will be made to proceed forward in compliance with PDD 63.

Results of your audit, as part of Phase III of the PCIE review on physical critical infrastructures, show adequacy of the Department's plans and actions taken to protect physical assets and facilities in accordance with PDD 63. However, the following recommendations, as a result of your findings, were identified within the audit that showed additional work must be forthcoming to ensure adequate physical security protection for all U. S. Department of Agriculture (USDA) facilities.

Recommendations

1. Work with USDA agencies to generate a listing of USDA-owned and commercially leased facilities and use this listing to identify mission essential facilities (or MEI) owned and leased by USDA.

   CORRECTIVE ACTION: OPPM has made contact with key USDA personnel in identifying all USDA owned and leased facilities. Representatives from APHIS, ARS, and FS, the largest landholding/leasing agencies within USDA, have been contacted directly and were requested to submit a listing of all owned and leased buildings within their purview. All facilities are being cross-referenced with available real property records currently existing in OPPM to ensure all facilities are identified and located. The Minimum Essential Infrastructure (MEI) will then be sorted out from the overall list of

ATTACHMENT A – OPPM RESPONSE

facilities. An inspection schedule will then be developed to visit these sites and conduct Threat Assessments (TA). These TA's will provide a guideline for any recommended security countermeasures that may be needed to ensure a facility is property secured. The list of facilities, identified as MEI, and the schedule to visit the sites to conduct a TA will be completed by December 2001. We will provide your office a copy of all information.

2. Pursue additional funding to ensure adequate resources and staff with the necessary skills is available to perform needed vulnerability assessments of critical USDA facilities and to carry out other necessary provisions of PDD 63.

   CORRECTIVE ACTION: OPPM will pursue additional funding to ensure adequate resources and staff with the necessary skills is available to perform needed vulnerability assessments of critical USDA facilities and to carry out other necessary provisions of PDD 63. However, please keep in mind that current funding and resources are limited, and there is no guarantee of increases in the immediate future. We are developing policies and procedures to conduct security assessments of all USDA facilities, and are working closely with the agencies to assist them in conducting TA's of their facilities and providing us appropriate documentation. We will forward a copy of these draft policies and procedures to you no later than October 31, 2001.

3. Include provisions in the security policies being developed for criteria to determine when a security or infrastructure-related incident should be reported to NIPC and procedures for reporting such incidents.

   CORRECTIVE ACTION: OPPM will include provisions in the security policies being developed to determine when a security or infrastructure-related incident should be reported to NIPC and procedures for reporting such incidents. As stated above in recommendation #2, we will provide a copy of our draft policies to your office no later than October 31, 2001.

OPPM appreciates the professional review and recommendations provided and look forward to working together in making USDA as safe a working environment as possible. If there are any questions regarding the corrective actions to be taken to comply with the recommendations in your audit report, please contact me at 202-720-9448 or have a member of your staff contact Richard C. Holman at 202-720-3901.