Office of Inspector General
Office of Audit

Department of Labor Is Refocusing Efforts to Improve Physical Security of its Minimum Essential Infrastructure

Report Number: 23-01-002-07-711
Date Issued: July 20, 2001

Table of Contents

Executive Summary

The Office of Inspector General (OIG) audited the Department of Labor's (DOL) efforts to protect its physical minimum essential infrastructure (MEI) as it relates to Presidential Decision Directive (PDD) 63 issued May 1998. PDD 63 calls for a national effort to assure security of the Nation's MEI which encompasses those physical and cyber-based systems essential to the minium operations of the economy and government. The audit was done in accordance with Government Auditing Standards issued by the Comptroller General of the United States and the President's Council on Integrity and Efficiency (PCIE)/ Executive Council on Integrity and Efficiency (ECIE) *Review Guide Phase III - Planning and Assessment Activities for Physical Minimum Essential Infrastructure.*

The Department's efforts to protect its identified MEI, since implementation of PDD 63, was found to be outdated and limited in focus. For example, the Department's Critical Infrastructure Protection Plan, (CIPP) dated June 1999, was not kept current with major revisions to the inventory of critical cyber PDD 63 systems and related physical facilities. In addition, the Department relied on assessments and/or surveys conducted by other Federal Government interests, such as the General Services Administration (GSA). However, recent efforts by the Department and specific departmental actions taken during OIG's audit fieldwork show that DOL efforts to protect its physical MEI are improving in the three key areas (i.e., critical infrastructure planning, identification of critical assets, and vulnerability assessments). The Department has developed a proactive approach to take specific steps to meet the requirements of PDD 63 and improve upon each of the three key areas.

To ensure the Department is prepared to meet potential threats against its physical MEI and meet the requirements of PDD 63, we recommend that the Assistant Secretary for Administration and Management take the following actions.

1. Foster an effective working relationship between the Chief Information Officer (CIO) and Business Operations Center to develop and complete a comprehensive CIPP which addresses all of its critical, physical (non-cyber based) MEI including identifying its:

    a. internal and external critical, physical (non-cyber based) MEI which are vital to the Department's operations (includes people and facilities) and the methodologies (processes) used to identify the buildings as critical, physical (non-cyber based) MEI of the Department; and

    b. associated interdependencies.

2. Establish policies and procedures for:

   a. governing the management and protection of the Department's MEI;

   b. evaluating new assets to determine if they need to be included as part of the MEI; and

   c. conducting periodic updates and evaluations of risk mitigation steps to determine if related policies, procedures and controls require updating.

3. Establish milestones for incorporating its Critical Infrastructure Protection (CIP) function into its strategic planning and performance measurement frameworks.

4. Include a reference in the CIPP to the Continuity of Operations Plan (COOP) and/or Continuation of Government (COG) plans as documents for the reestablishment of operations following an attack on its physical structures. Design, develop, and implement these related systems to fully respond to significant infrastructure attacks, while the attack is under way, with the goal to isolate and minimize damage to its MEI.

5. Conduct vulnerability assessments on all its critical, physical (non-cyber based) MEI for:

   a. identifying the current level of protection in place for its critical, physical (non-cyber based) MEI and the actions that must be taken before it can achieve a reasonable level of protection for its critical, physical (non-cyber based) MEI;

   b. prioritizing the threats according to their relative importance;

   c. identifying its vulnerabilities of its critical, physical (non-cyber based) MEI as it relates to its interdependencies with Federal agencies, state and local government activities and other infrastructure services; and

   d. develop an implementation plan and mechanism to monitor.

6. Adopt a multi-year funding plan to address the identified threats and the cost of implementing a multi-year vulnerability redemption plan in its budget submission to the Office of Management and Budget (OMB). Develop an estimate of the replacement costs, planned life-cycle, and potential impact to the Department if the asset is rendered unusable.

- - - - - - - - -

Based on discussions with departmental officials, response to the draft report, and receipt of information on planned corrective actions, the OIG has resolved all of the above recommendations and will continue to work closely with your office to bring each to closure.

Background

Presidential Decision Directive (PDD) 63, issued in May 1998, requires a national effort to assure the security of the Nation's critical infrastructures. Critical infrastructures are 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.

Under this directive, the United States Government and private business sector partners are required to take all necessary measures to eliminate any significant vulnerabilities to both physical and cyber attacks on our Nation's's critical infrastructures. PDD 63 requires that 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
- private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial and transportation services.

The PCIE/ECIE developed a four-phased initiative to determine the magnitude and extent government agencies have been addressing the elements of protecting its critical infrastructure. A description of the PCIE/ECIE's approach by review phase is summarized as follows (Phase III is highlighted as it is the focus of this report).

Phase I: Review the adequacy of agency *planning and assessment* activities for protecting its critical, *cyber-based* infrastructures. Specifically, review the adequacy of agency plans, asset identification efforts, and initial vulnerability assessments.

Phase II: Review the adequacy of agency *implementation* activities for protecting its critical, *cyber-based* infrastructures. Specifically, review the adequacy of agency activities in the following areas: risk mitigation; emergency management; interagency coordination; resource and organizational requirements; and recruitment, education and awareness.

Phase III: Review the adequacy of agency *planning and assessment* activities for protecting its critical, physical (*non-cyber-based*) infrastructures. Specifically, review the adequacy of agency plans, asset identification efforts, and initial vulnerability assessments.

Phase IV: Review the adequacy of agency *implementation* activities for protecting its critical, physical (*non-cyber-based* infrastructures). Specifically, review the adequacy of agency activities in the following areas: risk mitigation; emergency management; interagency coordination; resource and organizational requirements; and recruitment, education and awareness.

Objective, Scope, Criteria and Methodology

The overall objective of the OIG was to review the DOL's efforts to adequately protect its physical MEI. The OIG, through interviews and documentation analysis, assessed the adequacy of the DOL's planning and assessment activities for protecting its critical, physical (non-cyber based) infrastructures. Specifically, this involved the analysis of the adequacy of DOL's plan, asset identification efforts, and initial vulnerability assessments.

The scope of the work included DOL MEI as it is related to critical, physical (non-cyber based) MEI as defined by PDD 63 and covered the period of January 8, 2001 through April 5, 2001.

The audit was done in accordance with Government Auditing Standards issued by the Comptroller General of the United States and the PCIE/ECIE Phase III Review Guide dated October 25, 2000. In addition, OIG used principal Federal guidelines and provisions issued by the White House, OMB, Critical Infrastructure Assurance Office (CIAO), and the PCIE/ECIE, including: PDD 63, White Paper on PDD 63, the CIAO National Plan for Information Systems Protection and the PCIE/ECIE Schedule of Review Results.

The OIG, through interviews and documentation analysis, assessed the DOL's planning and assessment activities for protecting its critical, physical (non-cyber based) infrastructures. Specifically, this involved the analysis of the adequacy of DOL's plan, asset identification efforts, and initial vulnerability assessments.

Finding and Recommendations

Department Recognizes Identified Deficiencies in Three Key Physical Security Areas and Efforts are Under Way to Improve

The information in the Department's CIPP related to the critical physical MEI is outdated and limited and may result in unknown vulnerabilities due to the deficiencies identified in three key areas:

- Critical Infrastructure Planning
- Identification of Critical Assets
- Vulnerability Assessments

The Department has recognized these deficiencies and has developed a specific proactive approach to bring it into compliance with PDD 63 requirements.

Critical Infrastructure Planning is Outdated and Limited - Critical infrastructure planning includes the development and completion of a plan to protect critical, physical infrastructures. Physical security refers to the protection of building sites and equipment from theft, vandalism, natural and man-made disasters and accidental damage. The Department prepared a Critical Infrastructure Protection Plan (CIPP) dated June 10, 1999. However, the CIPP's focus is on the cyber MEI and while subsequent changes occurred to cyber and physical MEI, the CIPP was not correspondingly updated.

OIG's review determined that the Department did not have a CIPP that was accurate and current. Some of the Department's key activities and efforts toward development of a CIPP that addressed physical security are summarized below.

> **February 1999** - Department submitted its original CIPP to the CIAO's Expert Review Team (ERT) for review and comments.
>
> **February 1999 -** The ERT provided general and specific comments to the Department on the status of the CIPP. The ERT review contained general and specific comments related to the Department's CIPP. For example, one general comment for the Department from the ERT stated: *"Pages 1, 5 indicate that the CIPP requirements for physical protection have been deferred by GSA. PDD 63 requires that physical protection be addressed in the CIPP." The ERT recommended the essential infrastructure (including physical facilities, information systems, and personnel) needed to accomplish those missions, and an analysis and rationale of why the assets are essential to accomplishing critical agency missions be identified.*

June 1999 - The Department revised the February 1999 CIPP. OIG's review of the revised CIPP dated June 1999 determined it included an inventory of the Department's critical cyber and physical MEI assets. However, there was no evidence or mention in the CIPP of how or what the Department used to identify its critical, physical (non-cyber based) MEI.

February - April 2001 - The Department informed the OIG during its fieldwork that the Department was in the process of developing a draft CIPP which covers its critical, physical (non-cyber based) MEI and may lead to new policies and procedures for the Department of Labor. During the preparation of this report, the Department provided to the OIG a draft CIPP dated May 11, 2001, in response to their milestone date of May 8, 2001. The final CIPP should include the following:

- procedures for conducting periodic updates to determine if assets need to remain as Minimum Essential Infrastructure;
- development of mitigation plans for physical critical assets;
- information on physical redemption plans;
- channels of notification to internal and external organizations, including OIG criminal investigators, FBI and other relevant agencies of an infrastructure attack or attempts; and
- channels of communications and criteria for reporting and obtaining information on non-cyber attacks to the FBI's National Infrastructure Protection Center (NIPC).

A final CIPP will enable the Department to establish responsibilities and direct specific activities to ensure the protection of its critical, physical (non-cyber based) MEI assets.

Identification of Critical Assets is Outdated and Limited - Critical infrastructures are systems and assets - both physical and cyber - so vital to the Nation that their incapacity or destruction would have a debilitating impact on national security, national economic security, and/or national public health and safety. The Department's CIPP did not accurately account for the cyber and physical MEI assets as revisions were made to the asset inventories.

OIG's review of the Department's June 1999 CIPP determined it included an inventory of its critical cyber and physical MEI assets (i.e., 51 cyber MEI assets (12 general support systems, 39 major applications) and 73 related physical MEI assets). However, there was no evidence or mention in the CIPP of how or what the Department used to identify its critical, physical MEI assets. The break down of the physical MEI by owners is as follows:

Physical Inventory	Owner
53	GSA Owned
15	Commercial
1	GSA Owned/Leased
2	DOL Owned
1	National Institute of Occupational Safety and Health
1	Department of Defense
73	Total

The Department continued to make major revisions after June 1999 to its inventory of critical cyber PDD 63 systems but did not make corresponding revisions to its related physical facilities nor update the CIPP accordingly. In the agency's status report to the OIG, dated March 30, 2001, it states the inventory of critical physical facilities was developed based on facilities that housed components of the critical cyber-based assets. However, the CIPP did not provide, nor has OIG received, any evidence to indicate the Department had:

- identified milestones when the identification of its critical, physical (non-cyber based) MEI is to be completed;
- information on whether the identified critical, physical (non-cyber based) MEI included people and facilities;
- identified interdependencies for its critical, physical (non-cyber based) MEI; and
- determined the estimated replacement cost, planned life-cycle, and potential impact to the agency if the asset is rendered unusable.

Without an accurate identification of these assets in the CIPP, the Department would be unaware of what MEI needs protection.

Vulnerability Assessments are From External Sources - Vulnerability assessments determine the adequacy of security measures, identify security deficiencies, evaluate security alternatives, and verify the adequacy of such measures after implementation. Vulnerability assessments can provide the Department information on where the vulnerabilities exist and aid in the development of remediation plans to correct the identified vulnerabilities. There was no evidence in the CIPP to indicate vulnerability assessments were performed or being scheduled for each of the critical, physical MEI assets, except for continued assessments and/or surveys by external Federal Government interests (e.g., GSA).

In discussions with agency representatives, OIG determined *external* vulnerability assessments and/or surveys have been conducted on the critical, physical MEI. The external vulnerability assessments and/or surveys of Federal buildings had been performed by the Department of Justice (DOJ), GSA, and an investigation undertaken by the House Subcommittee on Crime.

The DOL's key physical security activities have included several physical security reviews and investigations by the GSA, DOJ, and special interest groups covering the period from 1992 to 2001.

OIG determined, based on the analysis of GSA's surveys/risk assessments and discussions with management staff, the Department has and continues to take steps to upgrade the Frances Perkins Building (FPB) as recommended by GSA. For example, the Department hired more guards to operate the security equipment. However, OIG has not received evidence to indicate the Department has conducted any vulnerability assessments and/or surveys on DOL owned and/or leased (commercial) property. The specific locations of these facilities are known to OIG and are not included in this report.

Without vulnerability assessments and/or surveys on DOL owned and/or leased facilities, the Department cannot:

- prepare redemption plans to address the vulnerabilities found during the assessment,
- determine level of protection currently in place for its physical (non-cyber based) MEI,
- identify actions that must be taken before it can achieve reasonable level of protection for its physical (non-cyber based) MEI,
- develop a related implementation plan and mechanism to monitor such implementation,
- adopt a multi-year funding plan to address the identified threats,
- reflect the cost of implementing a multi-year vulnerability redemption plan in its budget submission to OMB,
- prioritize threats according to their relative importance,
- assess the vulnerability of its physical (non-cyber based) MEI to failures that could result from interdependencies,
- develop a process to identify and reflect new threats to the Department's physical (non-cyber based) MEI, and
- determine if results necessitate revisions to departmental policies that govern the management and protection of the Department's physical (non-cyber based) MEI.

Efforts Now Under Way to Improve Focus on Key Physical Security Areas - In written response to OIG's field work, the Department is taking a proactive approach to address all three key areas of concern to ensure protection of its critical, physical (non-cyber based) MEI in the context of PDD 63. This proactive approach includes:

- developing a draft CIPP which covers its critical, physical (non-cyber based) MEI for the three key elements of critical infrastructure planning, identification of critical assets, and vulnerability assessments;

- obtaining copies of DOL agencies' vulnerability assessments performed on each of the critical, physical assets;

- implementing a new policy requiring agencies to provide the DOL Security Office with a copy of the assessments; and

- analyzing and reviewing the vulnerability assessments to make recommendations in areas deemed necessary to achieve an acceptable level of protection for its critical, physical infrastructure assets.

Conclusion

We found the Department's efforts to protect its identified MEI, since implementation of PDD 63, to be outdated and limited in focus. The Department's past approach to protecting its physical security assets has been to provide levels of protection based on recommendations of other Federal Government interests such as the GSA and the DOJ. During our audit work, the Department established a proactive approach to refocus its efforts through the development or update of its related security planning documents, asset inventory, and vulnerability assessments. Upon completion of these efforts, the Department will meet the requirements of PDD 63.

Recommendations

To ensure the Department is prepared to meet potential threats against its physical MEI and meet the requirements of PDD 63, we recommend that the Assistant Secretary for Administration and Management take the following actions.

1. Foster an effective working relationship between the CIO and Business Operations Center to develop and complete a comprehensive CIPP which addresses all of its critical, physical (non-cyber based) MEI including identifying its:

    a. internal and external critical, physical (non-cyber based) MEI which are vital to the Department's operations (includes people and facilities) and the methodologies (processes) used to identify the buildings as critical, physical (non-cyber based) MEI of the Department; and

    b. associated interdependencies.

2. Establish policies and procedures for:

    a. governing the management and protection of the Department's MEI;

    b. evaluating new assets to determine if they need to be included as part of the MEI; and

    c. conducting periodic updates and evaluations of risk mitigation steps to determine if related policies, procedures and controls require updating.

3. Establish milestones for incorporating its CIP function into its strategic planning and performance measurement frameworks.

4. Include a reference in the CIPP to the Continuity of Operations Plan (COOP) and/or Continuation of Government (COG) plans as documents for the reestablishment of operations following an attack on its physical structures. Design, develop, and implement these related systems to fully respond to significant infrastructure attacks, while the attack is under way, with the goal to isolate and minimize damage to its MEI.

5. Conduct vulnerability assessments on all its critical, physical (non-cyber based) MEI for:

    a. identifying the current level of protection in place for its critical, physical (non-cyber based) MEI and the actions that must be taken before it can achieve a reasonable level of protection for its critical, physical (non-cyber based) MEI;

    b. prioritizing the threats according to their relative importance;

c. identifying its vulnerabilities of its critical, physical (non-cyber based) MEI as it relates to its interdependencies with Federal agencies, state and local government activities and other infrastructure services; and

d. develop an implementation plan and mechanism to monitor.

6. Adopt a multi-year funding plan to address the identified threats and the cost of implementing a multi-year vulnerability redemption plan in its budget submission to OMB. Develop an estimate of the replacement costs, planned life-cycle, and potential impact to the Department if the asset is rendered unusable.

Acronyms

CIAO	Critical Infrastructure Assurance Office
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CIPP	Critical Infrastructure Protection Plan
COOP	Continuity of Operations Plan
COG	Continuation of Government
DOJ	Department of Justice
DOL	Department of Labor
ERT	Expert Review Team
FPB	Frances Perkins Building
GSA	General Services Administration
MEI	Minimum essential infrastructure
MSHA	Mine Safety and Health Administration
OIG	Office of Inspector General
OMB	Office of Management and Budget
PCIE	President's Council on Integrity and Efficiency
PDD	Presidential Decision Directive

U.S. Department of Labor

Office of the Assistant Secretary
for Administration and Management
Washington, D.C. 20210

JUN 20 2001

MEMORANDUM FOR JOHN J. GETEK

FROM: PATRICK PIZZELLA
Assistant Secretary for
Administration and Management

SUBJECT: Response to Draft Report No. 23-01-002-07-711
The Department of Labor is Refocusing
Efforts to Improve Physical Security of its
Minimum Essential Infrastructure

This memorandum responds to your May 31 draft audit report of DOL's efforts to improve the physical security of its minimum essential infrastructure. We have reviewed the draft report and agree with its findings and recommendations. As the draft report reflects, we have made solid progress in our efforts to protect DOL's critical infrastructure, specifically in the areas of critical infrastructure planning, identification of critical assets, and vulnerability assessments. DOL's draft Critical Infrastructure Protection Plan (CIPP), a copy of which was recently provided to your office, is an indication of the proactive approach we have been taking to meet the requirements of Presidential Decision Directive 63 (PDD-63). Among other things, PDD-63 requires agencies to develop a plan for protecting their own critical infrastructures, including but not limited to their cyber-based systems.

We also recognize that additional steps must be taken to ensure that DOL is fully prepared to meet potential threats against its essential infrastructure. Our Business Operations Center is working closely with the Deputy Chief Information Officer and DOL agencies to build on and enhance the draft CIPP, to ensure that the final Plan effectively addresses all of the requirements of PDD-63. We are in the process of refining a timetable of important milestones for this effort, which will provide your with our formal response to the final audit report.

If you have any questions or need additional information, please contact Al Stewart at (202) 693-4021.