September 28, 2001

MEMORANDUM FOR: PATRICK PIZZELLA
Assistant Secretary
for Administration and Management
Chief Information Officer

/s/

FROM: JOHN J. GETEK
Assistant Inspector General for Audit

SUBJECT: The Office of the Chief Information Officer Needs to Update Its Critical Infrastructure Protection Plan (CIPP)
Final Letter Report No. 23-01-003-04-433

This final letter report evaluates the actions taken by the Office of the Chief Information Officer (OCIO) to address Presidential Decision Directive 63 (PDD-63) – "Protecting America's Critical Infrastructure." In addition, the report includes in its entirety the response to the draft report by the Deputy Assistant Secretary of Operations for Administration and Management.

The Office of Inspector General's (OIG) objectives were to:

- verify that Department of Labor (DOL) had a reliable and documented process to identify critical information systems falling under the requirements of PDD-63; and

- verify what related actions DOL management have taken to date, or will take, to maintain an up-to-date inventory of critical physical assets and automated information systems to comply with PDD-63.

The scope of the audit included:

- reviewing the CIPP, the Cyber Security Program Plan (CSPP), OCIO's tracking documentation of system selection for PDD-63 purposes, and related OCIO and DOL agency PDD-63 correspondence;

- interviewing OCIO staff members to gain an understanding of the OCIO efforts to date in complying with PDD-63 and other DOL security requirements;

- meeting with DOL agency staff to gain an understanding of the efforts they have taken to date to comply with the PDD-63 requirement; and

- performing follow-up work in response to management concerns that OIG did not obtain all necessary documentation from the OCIO and discuss the Department's PDD-63 process more in-depth with the Director of ITC.

We conducted our audit between October 2000 and January 2001, and our follow-up work was performed between April 9-13, 2001. The work was performed in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States.

Background

PDD-63 calls for a national-level effort to assure the security of the Nation's critical infrastructure assets, both physical and cyber-based. The cyber-based critical infrastructures are those systems and their associated assets so vital to the Nation that their incapacity or destruction would have a debilitating impact on national security, national economic security, national public health and safety, and public confidence.

PDD-63 directs Departments and Agencies to develop CIPPs. Departments and agencies with the highest priority systems, designated as Phase One Agencies, were to have completed their initial plans in November 1998. These initial plans were followed by the Phase Two Agencies' (i.e., DOL, Department of Agriculture, Department of Education, Department of Housing and Urban Development, Department of Interior, General Services Administration, National Aeronautics and Space Administration, and Nuclear Regulatory Commission) plans that were to have been completed in February 1999 and implemented within two years. The Director, National Critical Infrastructure Assurance Office (CIAO), told the President's Council on Integrity and Efficiency (PCIE)/Executive Council on Integrity and Efficiency (ECIE) working group members that *all agencies are subject to PDD-63*.

The purpose of the CIPP is to develop a coherent, achievable department-wide strategy to fulfill the requirements of PDD-63. The initial step and the single most important component in developing and implementing a CIPP is the identification of critical infrastructure assets. This process includes determining the information systems, data, facilities, equipment, and personnel that constitute a department's or agency's critical information infrastructure.

For the purpose of assisting Federal agencies in identifying critical infrastructure assets, the CIAO has issued the following: *Practices for Securing Critical Information Assets, The Infrastructure Asset Evaluation Survey, and Project Matrix.*

Finding, Conclusion and Recommendations

Finding

We determined that while there was a process and some documentation for eventually identifying nine (9) major applications and three (3) general support systems as DOL critical information assets, this process may have resulted in the Department excluding other major applications and general support systems that are important to the health of the nation's economy, and to the functioning of the DOL.

To better manage its critical infrastructure assets, the OIG recommends the Chief Information Officer continue to work with the Critical Infrastructure Assurance Office's (CIAO) Project Matrix Team to conduct a further review of DOL's critical assets. This process should be formally documented and risk-based and result in an updated DOL Critical Infrastructure Protection Plan (CIPP) that will cover people, facilities, and cyber systems, as appropriate.

The Department's PDD-63 system selection process was found to be lacking:

- a cohesive strategy that leads to the identification of the critical infrastructure assets.
- a selection process that can be traced to reliable results from a documented risk-based review.
- an assessment of a program's mission to determine the ranking of the criticality of the PDD-63 assets.

The Department's process, instead, involved iterative efforts that reduced the number of PDD-63 systems from 51 to a number more in line with the requirements spelled out in guidance from the CIAO. The Department initially identified 39 major applications and 12 general support systems using the General Services Administration's *Draft Federal Sector Critical Infrastructure Protection Plan*. In examining the whole process that resulted in identifying the current nine major applications and three general support systems it was found that there was limited or no information available to show that a formal risk-based process had been used to identify PDD-63 application and general support systems.

The chronology of DOL's actions, which resulted in a reduction of the PDD-63 systems, is as follows:

1998 - The Department had taken a number of actions to identify DOL major applications and general support systems for purposes of managing the Department's critical infrastructure assets. These actions included (1) contracting technical support to help review, analyze, and develop DOL Information Security Plans; (2) forming the Critical Infrastructure Protection Working Group (CIPWG) to develop and implement the CIPP; (3) providing DOL agencies with the definition of "critical asset" from PDD-63 and asking the agencies to submit to the CIO their "critical assets" that would need security protection in accordance with the asset identification approach detailed in the CIPP; and (4) submitting draft copies of the Department's CIPP to the CIAO for review and evaluation and in having ongoing discussions with the CIAO.

June 1999 - DOL's CIPP originally designated 39 major applications and 12 general support systems as DOL critical systems for PDD-63 purposes. The approach used to identify critical infrastructure asset identification was based upon GSA's Draft Federal Sector Critical Infrastructure Protection Plan, dated October 7, 1998. Each DOL organization was to evaluate its applications and general support systems in accordance with the following GSA guidance: (1) Impact on Public Safety and Health; (2) Impact on Economic Security; and (3) DOL Business Functions.

August 1999 - Interaction occurred between the OCIO and CIAO. For example, the following comment was made in a letter, dated August 12, 1999 to Patricia Lattimore, from the Expert Review Team of the CIAO: *We commended the Department for the progress it was making in strengthening the Plan. Please continue to furnish the CIAO with revisions of the Plan when significant changes are made. . . .*

October 1999 – The Department's CIO issued DOL Cyber Security Plan on October 22, 1999. The Plan emphasizes that DOL is increasingly reliant on cyber systems while at the same time the threats to those systems are on the rise. PDD-63 recognizes this relationship and requires all agencies to develop a CIPP for those cyber systems whose loss or misuse would result in a severe impact on the country's critical sectors. The CIPP, at this time, covered only 21 systems.

November - December 1999 - A decision was made to increase the number of systems from 21 to 22 (11 major applications and 11 general support systems). No other information was provided/obtained on this upward revision to the number of DOL major applications and general support systems being reported for PDD-63 purposes. During this period, additional discussions were being conducted between the OCIO and CIAO.

December 1999 - A decision was made by DOL, after a discussion with the CIAO, to further reduce the number of DOL applications that were to be designated by DOL as part of the PDD-63 universe. The number of DOL major applications was reduced from 11 to 9, and general support systems from 11 to 3. DOL noted that only a small portion of the 11 previously identified general support systems supported the associated major applications.

Present – The OCIO has added additional classification groupings for the security of the Department's major applications and general support systems. The Department's major applications and general support systems not being classified under PDD-63 are grouped under OMB A-130 security requirement, or a financial category due to changes to OMB Circular A-11 and receipt of additional OMB guidance. Each major application and general support system in the PDD-63, financial, and OMB A-130 groupings are required to comply with the identified DOL CSPP components. These components include: Policy and Guidelines, Risk Management, Contingency Planning, Vulnerability Analysis and Testing, Incident Reporting and Response, and Computer Security Awareness. The PDD-63 classified systems are the only DOL systems required to perform the additional step of Mitigation Planning.

Department's CIPP Not a Primary Focus for PDD-63 Process

Based upon our analysis, it appears that the DOL CIPP is no longer being fully implemented, as described in the version dated June 1999. When issued, the CIPP was described as a living document, and changes to its milestones, deliverables, and responsibilities for achieving the Secretary's goal to meet PDD-63 was expected to evolve into a formal DOL CIPP through time. According to OCIO staff, the CIPP is currently being readdressed at this time.

While the Black Lung system was determined to be a PDD-63 system, other systems with similar or even greater funds and beneficiaries associated with it are not. For example, the table below, shows data on annual benefits provided and the number of associated beneficiaries for the Black Lung, Longshore, and Federal Employees' Compensation systems:

DOL System / Application	Annual Benefits Provided	Number of Annual Cases	Classified as a PDD-63 System
Black Lung System	$460 Million	65,000 – 81,000	Yes
Longshore and Harbor Workers' Compensation System (LHWCS)	$621 Million (program also maintains over $2 Billion in securities)	84,000	No
Federal Employees' Compensation System (FECS)	$1.9 Billion	165,000	No

While the Longshore and Harbor Workers' Compensation and the Federal Employees' Compensation systems both provide greater annual benefits to a larger number of beneficiaries than the Black Lung system, neither program's system / application is being reported by the OCIO as a PDD-63 system.

Management Comments

The OCIO management stated that the application / system selection process for PDD-63 purposes has been, and could be in the future, an evolving process. They reported that there has never been clear guidance on criteria for selecting systems for a Federal agency similar to DOL. In addition, staff from the OCIO stated that their role is not to mandate which systems should be classified as a PDD-63 system / application, but instead to work with the various DOL agencies to ensure that the appropriate systems are selected and that both physical and cyber vulnerabilities associated with those systems / applications are eliminated or minimized. The OCIO staff reported that their office will continue to seek guidance from the CIAO in the identification of applications and general support systems that should comply with PDD-63.

Conclusion

The Department's approach in identifying DOL's PDD-63 systems, while commendable, needs to be re-evaluated in a manner that is well documented and reflects a reliable risk-base approach for identifying those physical and cyber-based systems essential to the minimum operations of the Department and its agencies. Without a documented, reliable risk-based approach for identifying such systems, the OCIO may not be protecting, in priority order, all the Department's major applications and general support systems, which are important for national economic security, national public health and safety, and public confidence.

Recommendations

We recommend the Chief Information Officer:

1. Work with the CIAO's Project Matrix Team (PMT) to identify and characterize accurately the assets and associated infrastructure dependencies and interdependencies that DOL requires to fulfill is most critical responsibilities.

2. Update the Department's CIPP, based on the PMT's work, to include all cyber-based systems and cyber-related physical assets critical to protecting its own infrastructure.

3. Ensure that the updating of the CIPP is fully documented and the results available for review.

4. In cooperation with the Department's Business Operations Center work to ensure that any changes to the CIPP's cyber-based systems result in a corresponding identification of the physical critical infrastructure assets related to those systems.

--- --- ---

The September 28, 2001, response by the Deputy Assistant Secretary of Operations for Administration and Management indicates that through the Project Matrix effort DOL does not have any cyber-based systems that are within the scope of PDD-63 and refers to the letter September 28, 2001, from CIAO's Project Matrix Team. However, OIG's review of the Team's letter indicates that the Team identified two assets having a potential impact on the national security, economic stability, or public health and safety of the United States. The assets are the Mine Safety and Health Administration and Occupational Safety and Health Administration. The Team recommended, and OIG agrees, that Mr. Pizzella, Mr. Larisky, and Mr. Henshaw should continue to work with the Team to ascertain the true criticality of the two assets. OIG believes this work should cover the related assets' infrastructure, i.e., people, facilities, and cyber systems, where applicable.

This final letter report is submitted for your comment. We request a written response to this report within 60 days. If you have any questions, please contact Robert Curtis, Director, Office of Information Technology Audits, on (202) 693-7001.

Attachment