U.S. DEPARTMENT OF COMMERCE
Office of Inspector General

PUBLIC RELEASE

OFFICE OF THE CHIEF INFORMATION OFFICER

Critical Infrastructure Protection: Early Strides Were Made, but Planning and Implementation Have Slowed

Inspection Report No. OSE-12680/August 2000

Office of Systems Evaluation

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Presidential Decision Directive (PDD) 63, issued in May 1998, called for a national effort to ensure the security of the nation's critical infrastructures, also known as minimum essential infrastructure (MEI). Critical infrastructures are the physical and cyber-based[1] assets essential to the minimum operations of the economy and government. Advances in information technology (IT) have caused infrastructures to become increasingly automated and inter-linked, and have created new vulnerabilities to human error, natural disasters, and physical and cyber-attacks.

Since the targets of attacks on our critical infrastructure would likely include facilities both in the private sector and in the government, eliminating our potential vulnerability requires a closely coordinated effort of the public and the private sectors. The Department has responsibility for planning and executing a program for securing protection of the assets it manages. The Chief Information Officer (CIO) is responsible for the Department's internal critical infrastructure program. To comply with the directive, the CIO developed a critical infrastructure protection (CIP) plan, identified the Department's critical infrastructure assets, and conducted vulnerability assessments of some of its assets.

The objectives of our review were to evaluate the Department's CIP plan, identification of assets, and vulnerability assessment of its cyber-based assets. We focused on the CIO's management of the Department's CIP program, with emphasis on the seven operating units containing the largest number of critical assets: The National Oceanic and Atmospheric Administration, Census Bureau, U.S. Patent and Trademark Office,[2] Bureau of Export Administration, National Institute of Standards and Technology, Bureau of Economic Analysis, and National Telecommunications and Information Administration. Our review was conducted as part of a President's Council on Integrity and Efficiency/Executive Council on Integrity and Efficiency joint review involving 20 other Offices of Inspector General and federal agencies.

We found that the Department made initial progress in implementing PDD-63 by developing a Department-wide CIP plan, identifying critical infrastructure assets, and initiating vulnerability assessments. However, the plan does not reflect the status of PDD-63 implementation and is not

[1]Cyber is a prefix used in a growing number of terms to describe new things that are being made possible by the spread of computers. For example, cyber-space is the non-physical terrain created by computer systems. Anything related to the Internet also falls under the cyber definition.

[2]We refer in this report to USPTO as an operating unit of the Department of Commerce. However, in March 2000, PTO was reestablished as USPTO, an agency of the United States, within the Department of Commerce. The agency remains under the policy direction of the Secretary of Commerce, but exercises independent control of its budget, personnel, procurement, and other administrative and management functions.

complete. We believe the inventory of critical infrastructure assets is not reliable because of significant limitations in the methodology used in establishing it. Also, less than 10 percent of assets have been recently assessed for vulnerabilities and no remediation (corrective action) plans have been developed.

The Department's CIP plan needs to be revised. Several elements of the plan are outdated or missing, and important milestones have slipped. The plan's omissions include requirements for evaluating new assets to determine whether they should be included as MEI, periodically updating vulnerability assessments, developing a system for responding to significant infrastructure attacks in progress, incorporating security planning procedures into the basic design of new programs that include critical infrastructures, incorporating CIP functions into the Department's strategic IT planning and performance measurement frameworks, and notifying OIG criminal investigators of infrastructure attacks. Also, progress in implementing the directive has been slower than expected because of a lack of funding for analyzing and reducing vulnerabilities. The Office of the CIO informed us during our review that it plans to revise the Department's CIP plan by November 2000. We recommend that the revised CIP plan include the updated and omitted components (see page 9).

The MEI asset inventory should be reevaluated. Although a systematic process was applied in formulating the inventory, data gathering was significantly limited. In most cases, asset managers were neither interviewed nor given adequate guidance on program criteria before filling out fairly complex survey questionnaires used to gather asset information. Operating unit officials most knowledgeable about the assets were seldom interviewed because of logistical problems in setting up interviews and because several concurrent CIP-related tasks were performed during the same time frame by the Department's CIP review team, limiting resources available for the inventory. As a result, some operating units do not believe that the inventory is accurate.

Establishing a reliable MEI inventory is an important part of the requirements of PDD-63 because the inventory forms the basis for subsequent activities, such as selecting assets with the highest suspected risk for further vulnerability assessment and taking remedial actions. We recommend that the Department reevaluate its MEI assets using a revised methodology that includes improved guidance and increased interaction with operating units (see page 14).

Vulnerability assessments, remediation plans, and budget justifications need to be completed. The Office of Management and Budget will not provide funding for critical infrastructure protection activities without detailed budget requests based on vulnerability assessments and remediation plans. Because of resource constraints, the Department has current vulnerability assessments for less than 10 percent of its MEI assets and has not developed any remediation plans. As a result, it has not been able to obtain funding for its internal activities. A $79.2 million budget request submitted to OMB for FY 2001 was denied because detailed remediation plans had not been prepared. This request included $3.6 million for conducting vulnerability assessments.

PDD-63 requires agencies to conduct vulnerability assessments and prepare remediation plans. The Department's slow progress is a result of having insufficient resources to conduct CIP activities. OMB has emphasized, however, that no new funding will be provided unless extremely detailed budget requests showing the cost of corrective actions are submitted. Because of the importance of ensuring that the Department's critical assets are protected and the nonavailability of funding to do so in the absence of these vulnerability assessments and remediation plans, we recommend that the CIO form internal assessment teams comprising personnel from the Department and the bureaus and hold operating units—supported by these teams—accountable for completing vulnerability assessments, remediation plans, and improved CIP budget justifications (see page 18).

In an August 7, 2000, response to our draft report, the CIO generally agreed with our findings and recommendations. However, while the CIO recognizes the merit of our recommendations, the response reiterates the lack of funding for CIP-specific activities as an impediment to the Department's progress in implementing the directive. The CIO stated that the Department's focus will be on the broader spectrum of IT security, which emphasizes systems that are most critical to the mission of the Department and includes most cyber-based MEI assets.

The CIO is initiating near-term actions to implement several of our recommendations. These actions include (1) improving guidance to operating unit personnel involved in vulnerability assessments and increasing their involvement in reevaluating the MEI asset inventory, (2) training departmental staff to perform vulnerability assessments and encouraging operating units to conduct self-assessments, (3) revising the MEI asset list, (4) revising target dates for completing CIP-related tasks, (5) incorporating CIP functions into the Department's IT strategic planning and performance measurement frameworks, (6) evaluating new assets to determine whether they should be included as MEI, and (7) preparing a memorandum of agreement for notifying OIG criminal investigators of infrastructure attacks. The CIO will make major revisions to the CIP plan and incorporate the remaining outdated or missing elements in the plan as resources permit.

The CIO also stated that the Department will prepare remediation plans for assets that have been assessed for vulnerabilities and require operating units to prepare remediation plans after future assessments. The remediation plans will be used to develop budget projections. The Department has included three NOAA IT security/CIP budget initiatives in its FY 2002 budget request to OMB: High Performance Computing, Gateway Legacy System, and Network Security. These initiatives include several priority MEI assets that support weather forecasting.

INTRODUCTION

Presidential Decision Directive (PDD) 63, issued in May 1998, called for a national effort to ensure the security of the nation's critical infrastructures, also known as minimum essential infrastructure (MEI).[1] Critical infrastructures are the physical and cyber-based[2] systems essential to the minimum operations of the economy and government. Critical infrastructures include telecommunications, banking and finance, energy, transportation, and essential government services. Advances in information technology have caused infrastructures to become increasingly automated and inter-linked, and have created new vulnerabilities to human error, natural disasters, and physical and cyber-attacks.[3] Figure 1 illustrates threats and potential damage to systems supporting federal operations.

In PDD-63, the President intends 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. By May 2003, as a national goal the United States is to have achieved the ability to protect its critical infrastructures from international 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.

According to PDD-63, any interruptions or manipulations of these critical functions must be brief, infrequent, manageable, geographically isolated, and minimally detrimental to the nation.

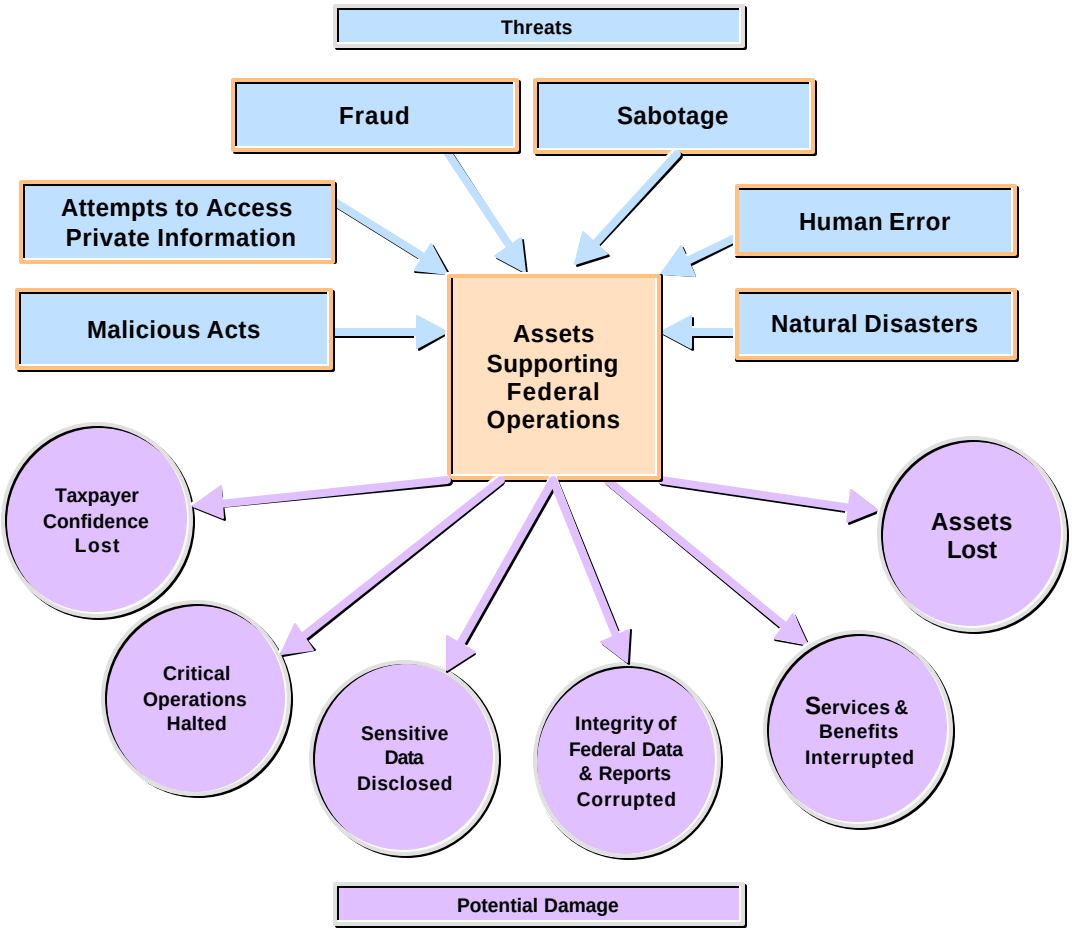
---

[1]An Administration white paper issued to explain the key elements of PDD-63 defines critical infrastructure as "...those physical and cyber-based systems essential to the minimum operations of the economy and government." The Critical Infrastructure Assurance Office has defined agency MEI as "the framework of critical organizations, personnel, systems, and facilities that are absolutely required in order to provide the inputs and outputs necessary to support the core processes essential to accomplishing an organization's core missions as they relate to national security, national economic security, or continuity of government services."

[2]Cyber is a prefix used in a growing number of terms to describe new things that are being made possible by the spread of computers. For example, cyber-space is the non-physical terrain created by computer systems. Anything related to the Internet also falls under the cyber definition.

[3]Cyber-attacks, or cyber-terror, may be defined as the unauthorized electronic access, manipulation, or destruction of electronic data or code that is being processed, stored, or transmitted on electronic media. The effect of these attacks can be actual or potential harm to the nation's critical infrastructure.

Figure 1. Information Security Risks Flowchart



Source: GAO

PDD-63 Implementing Structure and the Department's National Role

PDD-63 organizes the federal government into several components to meet the nation's security challenge:

- The **National Coordinator for Security, Critical Infrastructure, and Counter-Terrorism** at the White House National Security Council oversees national policy development and implementation for critical infrastructure protection. The National Coordinator, who is a member of the Cabinet-level Principals Committee, advises the President and the National Security Advisor on policy and implementation issues as they relate to our national critical infrastructures.

- The **Critical Infrastructure Assurance Office (CIAO)**, an interagency office housed at the Department of Commerce, supports planning with government agencies and the private sector. CIAO is also responsible for assisting agencies in identifying their dependencies on critical infrastructure, and coordinating a national education and awareness program, legislative issues, and public affairs.

- The **National Infrastructure Protection Center (NIPC)**, an interagency office at the FBI, serves as a threat assessment center focusing on threat warnings, vulnerabilities, and law enforcement. NIPC includes representatives from the FBI, the Department of Defense, the United States Secret Service, intelligence agencies, and other government agencies.

- Since the targets of attacks on our critical infrastructure would likely include facilities both in the economy and in the government, eliminating our potential vulnerability requires a closely coordinated effort of both the public and private sectors. For each infrastructure sector that could be a target for significant cyber or physical attacks, a single U.S. government department or agency serves as the **Lead Agency** for liaison. Each Lead Agency for a particular sector of the critical infrastructure has also designated a **Sector Liaison Official** to direct efforts in that sector. The Department of Commerce is among nine lead agencies for sector liaison, while four other agencies have responsibility for special functions, such as defense, law enforcement, and foreign issues. The Department is responsible for information and communications, as shown in Table 1.

- The Sector Liaison Officials work closely with the National Coordinator on the **Critical Infrastructure Coordinating Group (CICG)**, the interagency committee analyzing critical infrastructure policy issues and developing policy recommendations for the Cabinet-level Principals Committee.

Within the Department, the Bureau of Export Administration, National Telecommunications and Information Administration, and National Institute of Standards and Technology have important national roles in implementing PDD-63. BXA has oversight of CIAO, which reports to the Department's Under Secretary for Export Administration. NTIA is the sector lead for information and communications and is involved in critical infrastructure protection (CIP) education and awareness. The NTIA Administrator is the Sector Liaison Official**.** NTIA chairs the CICG Education and Awareness Committee, in which the government and private sector work together to increase national awareness of the importance of CIP.

NIST's mandate under PDD-63 is primarily research and development. NIST will house the Institute for Information Infrastructure Protection, which will be established in FY 2001 to fund, coordinate, and integrate information security research not being addressed through existing industry or government programs. See Appendix A for a list of specific NIST research areas.

Table 1. Lead Agencies for Sector Liaison Within the U.S. Government

Agency	Assignment of Responsibility
Department of Commerce	Information and Communications
Department of Energy	Electric Power, Oil, and Gas Production and Storage
Department of Health and Human Services	Public Health Services, Including Prevention, Surveillance, Laboratory Services, and Personal Health Services
Department of Justice/FBI	Emergency Law Enforcement Services
Department of Transportation	Aviation, Highways, Mass Transit, Pipelines, Rail, and Waterborne Commerce
Department of the Treasury	Banking and Finance
Environmental Protection Agency	Water Supply
Federal Emergency Management Agency	Emergency Fire Service and Continuity of Government Services
General Services Administration	Federal Government

NIST and the National Security Agency (NSA) have existing responsibilities under the Computer Security Act of 1987 to develop recommended practices for the federal government. Under PDD-63, NIST will work with NSA, the General Services Administration, OMB, and the National Coordinator to develop and implement best practices and standards for critical federal information systems by January 2001. NIST will also establish a permanent Expert Review Team (ERT) to replace the interim ERT at CIAO. The ERT will assist government agencies in adhering to federal computer security requirements. At an agency's request, NIST and NSA will perform independent analyses of critical federal information infrastructures and provide reports of their results to the agency's Chief Information Officer (CIO).

The budget submitted by the President to the Congress in February projected $52 million in estimated funding for Commere CIP-related activities in FY 2001. The lion's share, $48 million, is for the NIST Institute. NIST will provide research grants to industry and universities. Total funding for CIP for the Department for FY 1998 through FY 2000 is about $50 million. The Department's funding to date has

been for its national responsibilities.[4]

The National Plan

In January 2000, the President issued, *National Plan for Information Systems Protection, Version 1.0, An Invitation to a Dialogue*. This first version of the plan focuses on the federal government's domestic efforts to protect the nation's critical cyber-based infrastructures. Subsequent versions of the plan will incorporate a broader range of concerns contemplated under PDD-63, including the specific role that industry and state and local governments will play. The specific objectives and programs of the National Plan are listed in Appendix B.

Associated with objectives and programs in the National Plan are almost 80 milestones, most of which are scheduled to be completed by December 2000. Among the first milestones are instructions for each of the nine agencies listed in Table 1 to (1) perform initial vulnerability assessments[5] and develop remediation plans to fix vulnerabilities, and (2) submit a multi-year vulnerability remediation plan with their FY 2001 budget and annually thereafter.

Department of Commerce Internal Activities

The CIO is responsible for the Department's internal critical infrastructure as the appointed Chief Infrastructure Assurance Officer. In this position, the CIO manages PDD-63 implementation, which includes establishing procedures for obtaining expedient vulnerability assessments of the Department's critical infrastructure assets.

PDD-63 required federal departments and agencies, by November 1998, to develop a plan for protecting their critical infrastructure. The Department published its CIP Plan on schedule based on input from the operating units. The Department's CIP plan established objectives, approaches, deliverables, and milestones for identifying MEI, conducting vulnerability assessments, developing remediation plans, and other elements for implementing PDD-63.

A revised version of the plan was issued in April 1999 and incorporated several changes recommended by CIAO. This version also included a draft list of 31 MEI assets, budget requirements for CIP-related activities through FY 2004, and additional CIP milestones.

[4]OMB approved $4 million for securing NOAA's Advanced Weather Interactive Processing System. However, these funds were not specifically included in the Department's FY 2001 budget request for internal CIP activities.

[5]"Initial" vulnerability assessment is not defined in PDD-63. The Department considers that its effort to determine asset applicability to PDD-63 criteria and establish an MEI asset inventory satisfied the requirement for an initial vulnerability assessment.

Shortly after issuing its initial CIP plan, the Department hired a contractor to perform five tasks:

1. Independently verify and validate MEI asset choices.
2. Formulate the FY 2001 budget estimate for internal CIP-related activities.
3. Review the CIP plan and recommend improvements.[6]
4. Assess the state of security-related planning (as related to OMB Circular A-130, Appendix III, and the Clinger-Cohen Act) and Information Technology Strategic Planning.
5. Identify threats to CIP assets.

The contractor issued a report[7] on April 16, 1999, which addressed the first four tasks and included a revised list of 231 MEI assets and a prioritization of assets based on criticality.

OBJECTIVES, SCOPE, AND METHODOLOGY

In August 1999, the Federal Audit Executive Council met to discuss a model role for the Inspector General community in critical infrastructure assurance (see Appendix C). In September 1999, the President's Council on Integrity and Efficiency (PCIE) Audit Committee unanimously supported a proposal by the Council that the PCIE initiate a review of the nation's critical infrastructure assurance program.

The PCIE/Executive Council on Integrity and Efficiency (ECIE) developed a review guide based on four phases of review:

Phase I — Participating OIGs will review the adequacy of agency *planning and assessment* activities for cyber-based infrastructures. The review will cover agency plans, asset identification efforts, and initial vulnerability assessments.

Phase II — Participating OIGs will review the adequacy of agency *implementation* activities for cyber-based infrastructures including taking corrective actions; establishing emergency management policies and procedures; coordinating with interagency groups; defining and obtaining resource and organizational requirements; and recruiting, educating, and making people aware of CIP.

Phase III — Same as Phase I only for non-cyber-based infrastructures.

[6]The Department's revised CIP plan did not incorporate improvements recommended by the CIP contractor.

[7]*U.S. Department of Commerce, Department-Level Vulnerability Assessment, in Compliance with Presidential Decision Directive 63*.

Phase IV Same as Phase II only for non-cyber-based infrastructures.

This review covers Phase I, which aligns with the first objective of the National Plan: Prepare and Prevent, the steps necessary to minimize the possibility of a significant successful attack on MEI and to build an infrastructure that remains effective during attacks; and the first program of the National Plan: identify critical assets and shared interdependencies and address vulnerabilities (see Appendix B). We determined the adequacy of the Department's CIP plan and evaluated the methodology used by the Department to identify assets and conduct vulnerability assessments. Our specific objectives for Phase I and an explanation of how we accomplished our objectives follow.

1. **Critical Infrastructure Planning** - Determine whether the Department and bureaus have developed an effective plan for protecting their critical cyber-based infrastructures.

   To satisfy our first objective, we evaluated the November 1998 and April 1999 versions of the Department's CIP plan and the operating unit plans that support it. We compared the contents of the plan to criteria established in PDD-63 and determined whether suggested improvements recommended by the ERT and CIP contractor were incorporated in the plan.

2. **Identification of Critical Assets** - Determine whether agencies have identified their cyber-based MEI and interdependencies.

   We met our second objective by evaluating the basis used by the contractor to develop the MEI asset list. We also evaluated the changes to the asset identification methodology that are being made in preparation for the Department's reassessment of MEI later this year.

3. **Vulnerability Assessments** - Determine whether agencies have adequately (1) identified the threats, vulnerabilities, and potential magnitude of harm to their cyber-based MEI that may result from the loss, alteration, unavailability, misuse, or unauthorized access to or modification of their critical cyber-based infrastructure investments, and (2) developed remediation plans to address the risks identified.

   Our third objective involved determining the extent to which the Department's assets had been assessed for vulnerabilities and the scope, methodology, and date of the assessments. We also determined to what extent remediation plans had been developed based on vulnerability assessments and whether remediation information was used to justify budget resources to implement PDD-63. We did not independently verify the criticality of Departmental MEI assets or the specific vulnerabilities identified for the assets.

Our review focused on PDD-63 activities involving seven operating units that are responsible for the Department's top 57 assets defined by the CIP contractor as "most critical." These operating units also

account for 220 of the Department's current inventory of 241 PDD-63 Critical Assets and are listed in descending order of the number of assets for each operating unit:

1. National Oceanic and Atmospheric Administration (National Weather Service and National Environmental Satellite, Data, and Information Service).
2. Bureau of the Census.
3. U.S. Patent and Trademark Office[8].
4. Bureau of Export Administration.
5. National Institute of Standards and Technology.
6. Bureau of Economic Analysis.
7. National Telecommunications and Information Administration.

Our fieldwork was conducted at Department of Commerce headquarters in Washington, D.C., and involved interviews with the Department's CIP Program Manager, organizationally located in the Office of Information Planning and Review, Office of the CIO, and review of all pertinent CIP-related data. We conducted limited interviews with operating unit CIP points of contact in the Washington, D.C., area and collected some CIP documentation directly from the operating units. Our field work was conducted between January and April 2000.

This inspection was performed in accordance with the Inspector General Act of 1978, as amended, and the *Quality Standards for Inspections*, March 1993, issued by the PCIE.

We held an exit conference with the CIO/Critical Infrastructure Assurance Officer for the Department of Commerce on June 12 to discuss the results of our review. The CIO generally agreed with our findings and recommendations, but stressed the severe negative impact a lack of resources has had in implementing PDD-63 in the Department.

[8]We refer in this report to USPTO as an operating unit of the Department of Commerce. However, in March 2000, PTO was reestablished as USPTO, an agency of the United States, within the Department of Commerce. The agency remains under the policy direction of the Secretary of Commerce, but exercises independent control of its budget, personnel, procurement, and other administrative and management functions.

FINDINGS AND RECOMMENDATIONS

The Department made initial progress in implementing PDD-63 by developing a Department-wide CIP plan, identifying critical infrastructure assets, and initiating vulnerability assessments. However, the plan does not reflect the status of PDD-63 implementation and is not complete. We question the reliability of the inventory of critical infrastructure assets because of significant limitations in the methodology used in establishing it, and less than 10 percent of the Department's critical assets have been recently assessed for vulnerabilities.

To satisfy the requirements of PDD-63, the Department needs to revise its CIP plan, reassess its critical infrastructure asset inventory, and assess the vulnerabilities of additional assets. In order to obtain funding to mitigate its vulnerabilities, the Department needs to identify specific remedial actions to be taken.

I. Department's Critical Infrastructure Protection Plan Needs to Be Revised

The Department's April 1999 CIP plan establishes a general strategy for providing protection to the Department's MEI. However, the plan's usefulness is limited because important elements are not current or are missing. Also, important milestones have slipped.

A. Elements of the Plan Are Outdated or Missing

Several elements of the plan need to be updated. The plans's MEI list contains the original 31 assets identified by the Department, before the number of assets was expanded to 241. The original list employed a limited analytical methodology and does not reflect the Department's physical assets and most of its cyber-based assets. The vulnerability assessment framework referred to in the plan was replaced. As with the MEI asset list, the methodology envisioned for conducting vulnerability assessments changed as the Department expanded its analysis of CIP. The budget estimates for CIP-related activities are also outdated. These estimates were superseded by estimates developed in 1999 by the CIP contractor for formulating the FY 2001 budget for internal CIP activities.

Several elements are also missing from the plan. The plan does not include a provision for evaluating new assets to determine whether they should be included as MEI, nor does it require periodic updates of vulnerability assessments. In addition, the plan's emergency management element does not require that a system be developed to respond to significant infrastructure attacks in progress, or that OIG criminal investigators be notified of infrastructure attacks.

The plan also does not include a requirement that operating units incorporate security planning procedures into the basic design of new programs that include critical infrastructures. Such procedures would include provisions for risk management assessments, security plans for information technology

(IT) systems, identification of classified or sensitive information, and awareness and training measures to be taken for each program. Furthermore, the plan does not require that CIP functions be incorporated into the Department's IT strategic planning and performance measurement frameworks.

According to the Department, the purpose of the CIP plan is to satisfy the requirements of PDD-63 by establishing a path toward the cost-effective, efficient protection of its critical infrastructure. However, the significant number of outdated and omitted elements of the plan detract from its usefulness as a guide in implementing the directive. The Office of the CIO informed us during our fieldwork that it plans to update the CIP plan by November 2000 and include a revised asset inventory, vulnerability assessment framework, and budget.

The revised plan should include a requirement to evaluate new assets for inclusion as MEI as a recurring procedure for keeping the inventory current. If new assets are not evaluated with PDD-63 requirements in mind, they may not be given the level of protection needed. The Department's plan requires updates to the threat framework annually or as major events unfold. Equally important to maintaining asset protection is periodically updating vulnerability assessments on existing assets to ensure that the assets can respond to new or changing risks. PDD-63 encourages agencies to conduct frequent assessments of asset reliability, vulnerability, and threat environment due to rapid changes in technology and the nature of the threats to critical infrastructure.

PDD-63 also requires agencies to develop a system for responding to a significant infrastructure attack while it is underway, with the goal of isolating and minimizing damage. The FBI-operated NIPC will provide a national focal point for gathering information on threats to infrastructure. Additionally, NIPC will provide the principal means of facilitating and coordinating the federal government's response to an incident, mitigating attacks, investigating threats, and monitoring reconstitution efforts. The Department's system would be used for internal purposes and to cooperate with NIPC and provide any assistance, information, and advice that NIPC may request, including information on threats and warning of attacks, and about actual attacks on the Department's assets.

The plan states that incident data will be provided to NIPC and will be disseminated throughout the Department as appropriate. However, unless the OIG is specifically identified as an organization to be notified, agencies may not know to inform the OIG's criminal investigators of these incidents, and the Department's ability to respond to incidents may be compromised. According to Department Administrative Order 207-10, operating units must promptly report to the OIG the possible existence of violations of laws, rules, or regulations. The Inspector General Act of 1978, as amended, requires the Inspector General to keep the Secretary and the Congress fully and currently informed about problems and deficiencies relating to the administration of Department of Commerce programs and operations and the necessity for and progress of corrective action, and to report potential federal crimes to the Attorney General.

Security planning procedures should be included in the basic design of new programs that include critical infrastructures. OMB Memorandum M-00-07, *Incorporating and Funding Security in Information Systems Investments*, and Circular A-130, Appendix III, *Security of Federal Automated Information Systems*, require agencies to incorporate and fund security as part of agency IT systems and architecture, and to ensure that appropriate security controls are specified, designed into, tested, and accepted in computer applications.

The circular references specific guidance from NIST's *An Introduction to Computer Security: The NIST Handbook*, Special Publication 800-12, which devotes a chapter to security and planning in the computer system life cycle. The chapter points out that it costs 10 times more to add a security feature to a system *after* it has been designed than to include the feature in the system at the initial design phase. The handbook provides criteria for conducting sensitivity analyses for new systems by considering both the information to be processed and the system itself, determining security requirements and incorporating the requirements into systems, and providing system security accreditation that authorizes the explicit acceptance of risk in operational systems.

To ensure that strategic IT plans include consideration of CIP, the Department has been reviewing and commenting on operating unit strategic IT plans, and improvements in the plans have been noted. The Department also issued guidance that the plans cover CIP. The Department should further formalize this process by incorporating into its CIP plan a requirement for operating units to include CIP in their strategic IT plans. Strategic IT plans provide a structured process for thinking about how to apply technology to improve program services by providing descriptions of IT investments to be considered in the budget review cycle, including strategies to address IT security and critical infrastructure protection. OMB Circular A-130, Appendix III, section 3.a.2., requires agencies to incorporate summaries of security plans consistent with guidance issued by NIST into their strategic IT plans. The Computer Security Act of 1987, section 6.b., reiterates the requirement.

B. Important Milestones Have Slipped

The Department has made progress in implementing PDD-63, but is well behind its internal schedule and an optimistic schedule published in the President's National Plan. An initial CIP plan was published in November 1998 to comply with the first requirement of the directive. In April 1999, the Department published a revised version of the plan, an initial Department-level vulnerability assessment, a revised inventory of PDD-63 MEI assets, and an assessment of threats to the Department's MEI.

The Department's current milestones were developed for the original November 1998 plan, and carried forward to the April 1999 version without adjustment. Some of the plan's important milestones were scheduled to have been met by now, but have not been completed. According to the milestones, vulnerability assessments were to be completed by December 1999 and corresponding remediation

plans to correct asset vulnerabilities by February 2000. According to the National Plan, the Department should also have submitted a multi-year vulnerability remediation plan to OMB by June 1999, along with its FY 2001 budget request. None of these milestones are near completion. Hence, the milestones need to be updated with realistic completion dates for implementation.

The Department made substantial early progress in implementing PDD-63. The first Department-level CIP plan was issued within the 180-day time frame established by the directive, and a revised plan and the *Department-Level Vulnerability Assessment* were both issued in April 1999. Early activities also included the revised MEI inventory and assessment of the threats to the Department's MEI. The Department also assessed the vulnerability of 22 of its assets. In the last year, however, progress has been slow as reflected by the missed milestones. The Department explained that progress in implementing PDD-63 is behind schedule because it has not received funding for its internal CIP program activities.

PDD-63 requires CIP plans to have been implemented within two years and requires agencies to update the plans every two years. Implementation and an updated plan are both due in November 2000. Because important milestones have slipped, the CIP plan likely will not be implemented on time. The CIP Program Manager intends to update the plan by the November deadline.

C. Recommendation

We recommend that the Department's CIO:

1. Include in the Department's updated CIP plan:

    a. A revised MEI asset list that prioritizes assets.

    b. The revised framework for conducting vulnerability assessments.

    c. Current budget estimates for CIP-related activities.

    d. A provision for evaluating new assets to determine whether they should be included as MEI.

    e. A requirement to update vulnerability assessments.

    f. The development of a system for responding to significant infrastructure attacks in progress.

    g. A requirement to notify OIG criminal investigators of infrastructure attacks.

h. A requirement that operating units incorporate security planning procedures into the basic design of new programs that include critical infrastructure.

i. A provision for incorporating CIP functions into the Department's IT strategic planning and performance measurement frameworks.

j. Updated milestones, including milestones for revising the MEI asset inventory and completing vulnerability assessments and remediation plans.

D. CIO Response and OIG Comments

The CIO agrees that its CIP plan should be updated and kept up to date. However, given the lack of funds for CIP efforts, the workload of the IT security staff, and the critical need for IT security for Commerce mission-critical systems, the CIO feels that there are very limited resources to spend on rewriting the plan at this time. The CIO indicated that he will completely revise the plan when funds are available.

In the meantime, the CIO has agreed to make some adjustments in the near future. Specifically, the CIO is addressing or will address in the near future (1) revising the MEI asset list, (2) revising target dates for completing CIP-related tasks, (3) incorporating CIP functions into the Department's IT strategic planning and performance measurement frameworks, (4) evaluating new assets to determine whether they should be included as MEI, and (5) preparing a memorandum of agreement for notifying OIG criminal investigators of infrastructure attacks. The CIO also stated that the Department will prepare remediation plans for assets that have been assessed for vulnerabilities and require operating units to prepare remediation plans after future assessments. The remediation plans will be used to develop budget projections.

Elements that will be incorporated into a future major revision of the plan include (1) the revised framework for conducting vulnerability assessments, (2) a requirement to update vulnerability assessments, (3) the development of a system for responding to significant infrastructure attacks in progress, and (4) a requirement that operating units incorporate security planning procedures into the basic design of new programs that include critical infrastructure. The major revision to the CIP plan will be made as resources permit.

The CIO's complete response is included as Appendix E.

II. Minimum Essential Infrastructure Asset Inventory Should Be Reevaluated

We question the reliability of the MEI asset inventory because of weaknesses in the methodology used to gather asset data. Although a systematic process was applied in formulating the inventory, data gathering was limited because few asset managers were interviewed or given adequate guidance on program criteria.

In response to PDD-63, the Department initially identified an MEI asset inventory that included 31 cyber-based assets, but contrary to PDD-63 criteria, excluded physical assets. A contractor was hired to independently verify and validate the inventory. The contractor revised and expanded the list in April 1999 to 231 PDD-63 assets, including physical assets. The Department added another 10 assets after the list was expanded, bringing the total to 241. To prioritize the assets, seven ranking parameters[9] were developed and a weighting value[10] assigned to each. Weights were assigned by judging the relative importance of each parameter. The top 57 assets representing the top 25 percent of the original 231 assets were to receive vulnerability assessments and corrective actions first. The Department had planned to address all systems over a four-year period, 25 percent per year, from FY 2000 to the FY 2003 PDD-63 implementation deadline.

A survey questionnaire was used to collect asset data, but operating unit managers with direct responsibility for, and the most knowledge of, the assets were generally not interviewed. The original intent was that operating unit managers would be interviewed, and the survey questionnaires would be completed by the contractor during the interviews. However, there were logistical problems in arranging the large number of meetings with operating unit managers necessary to complete the questionnaires. Also, the CIP contractor completed several other CIP-related tasks (listed on page 6) during the same two-month period in which the asset inventory was completed, limiting resources available for the inventory. As a result, there was not enough time to meet and coordinate with the operating units, complete the surveys, or conduct thorough research on the assets.

Instead, operating unit managers were allowed to complete the survey questionnaires themselves. In only a few instances did the contractor interact directly with operating unit managers who completed the surveys. A significant number of surveys were not returned. For example, NOAA received 225

[9]The ranking parameters align generally with the national goal elements listed on page 1. The specific ranking criteria were the degree to which assets (1) perform essential national security missions, (2) ensure the general public health and safety, (3) provide valuable services to other government programs, (4) deliver minimum essential public services, (5) ensure the orderly functioning of the economy, (6) ensure the delivery of essential private sector services, and (7) maintain order.

[10]Weights for the ranking parameters ranged from 0.05 to 0.25, with the sum of all weight values equaling 1.00.

survey questionnaires but initially returned only 140, or 62 percent. In cases where the surveys were not returned, analyses were prepared using available information. The year 2000 critical systems inventories, strategic and operational IT plans, budgets, the Department's annual performance plan, and other information available from the Department's World Wide Web sites were researched and orientation interviews were conducted with senior Department officials to verify, validate, and expand the list from 31 to 231 PDD-63 assets. In the 13 months since the contractor finished its work, questionnaires were received for all but 8 assets and the Department expanded the inventory list to 241 assets.

The questionnaires that were returned had serious limitations. The questionnaires contained approximately 100 yes/no questions that were self-administered. Although this type of question is popular because of its simplicity, it has a significant drawback when used to identify critical assets. Yes/no questions are ideal for dichotomous variables, such and black and white, because they measure whether the condition or trait is present or absent. However, many of the questions asked of the operating unit officials dealt with measures that are not absolute or that span a range of values or conditions. Although this questionnaire design was not ideal for critical asset identification, the answers would have been more meaningful if the respondents had been given verbal or written guidance regarding the intent and exact meaning of the questions. Consider the question: "Does this asset support minimum essential standards for public services?" To answer the question, respondents need to know the definition of "minimum essential standards for public services." However, no definitions were provided with the questionnaire to aid respondents, and as noted above, few discussions were held.

Another problem with collecting asset data was that the operating unit respondents were given little guidance on who should complete questionnaires for asset identification, or how to fill them out. Some oral guidance was provided to high level managers, but not enough to ensure a consistent understanding of asset criteria among operating unit managers. As a result, some questionnaires were completed by security officers, who may not have been sufficiently knowledgeable about the uses of the assets. Also, some respondents viewed their assets from an internal mission perspective rather than considering their assets' implications on the national infrastructure because they did not fully understand program criteria. For example, one operating unit's responses were focused almost exclusively on its own internal mission.

Establishing the MEI inventory is an important part of the requirements of PDD-63 because the inventory forms the basis for subsequent activities. Based on the inventory, the assets with the highest suspected risk are given priority for further vulnerability assessment to determine the amount of risk exposure. A remediation plan can then be formulated to reduce the vulnerability. Remediation plans are also used to justify budget resources so that corrective actions can be implemented. If the inventory is not accurate, the Department's most vulnerable assets may not be recognized, and vulnerabilities may not be addressed in priority order. Three of the Department's largest operating units, NOAA, Census, and USPTO, have expressed concern that the inventory does not accurately reflect the priority of their assets.

Eliminating the interviews with operating unit managers significantly limited the value of the data gathered. The planning data used extensively by the Department in the absence of interviews does not necessarily include sufficient detail to determine whether the asset should be included in the MEI inventory. Interviews with asset managers could have provided more information about the assets and served as a mechanism for promoting communication about the asset, PDD-63 requirements and criteria, and the operating unit's role in critical infrastructure protection.

Guidance focused on PDD-63 criteria and the asset evaluation process could have aided survey respondents and resulted in a more accurate data gathering process and asset inventory. The Department should work closely with operating units to re-inventory the Department's PDD-63 assets. Assessment teams should include operating unit personnel who are the most knowledgeable about the asset's functions, dependencies, and end users.

In January 2000, CIAO issued *Practices for Securing Critical Information Assets* to provide guidance to federal agencies in identifying critical assets. The document includes a checklist that is an improvement over the questionnaire used by the Department because it explains variables and provides degrees of measure for questions. The Department has stated that it will use the CIAO questionnaire when it conducts another critical asset inventory.

A. Recommendation

We recommend that the Department's CIO:

2. Reevaluate the Department's Minimum Essential Infrastructure assets by the dates established in the updated Departmental CIP plan and include in the methodology:

    a. Increased involvement from operating units, including interviews with asset managers or others most knowledgeable about the asset's functions, dependencies, and end users.

    b. Improved guidance to operating personnel involved in assessments.

B. CIO Response and OIG Comments

The CIO agrees that the asset inventory needs further revision and will take near-term steps to refine the evaluation of those MEI assets previously identified as most critical. However, the CIO reiterates that funding and staff resources are limited. The CIO is using lessons learned from the first round of asset evaluations and recent CIAO guidance to improve the asset evaluation process, including the formation of teams of executives, managers, and technical experts from each asset under review to participate in training, interviews, and evaluations. The improved process will be used in the next round

of asset evaluations. Although the CIO stated that there is some operating unit resistence to the new process, CIO staff will work to correct what it believes is a misunderstanding of the process.

The CIO agreed that the guidance could be improved for the execution of the assessments and has taken an active part in developing the recently published CIAO methodology. The methodology will be used to improve the Department's process.

The CIO's complete response is included as Appendix E.

III. Vulnerability Assessments, Remediation Plans, and Budget Justifications Need to Be Completed

OMB will not provide funding for complying with PDD-63 until the Department conducts vulnerability assessments, then uses the results of the assessments to develop remediation plans and detailed budget formulations. Because the Department has not received funding for internal CIP activities, it has conducted recent vulnerability assessments for less than 10 percent of its MEI assets and has not developed any remediation plans.

A. Vulnerability Assessments and Remediation Plans Need to Be Completed

The Department has conducted vulnerability assessments[11] for only 22 of its 241 MEI assets since PDD-63 was issued in May 1998. Another 7 assessments are scheduled to be completed by July 2001. Figure 2 shows the status of asset vulnerability assessments for the seven Commerce operating units that account for 220 of the Department's 241 PDD-63 critical assets and contain the Department's top 57 assets defined by the CIP contractor as "most critical." Remediation plans[12] needed to justify CIP budgets based on completed vulnerability assessments have not been prepared.

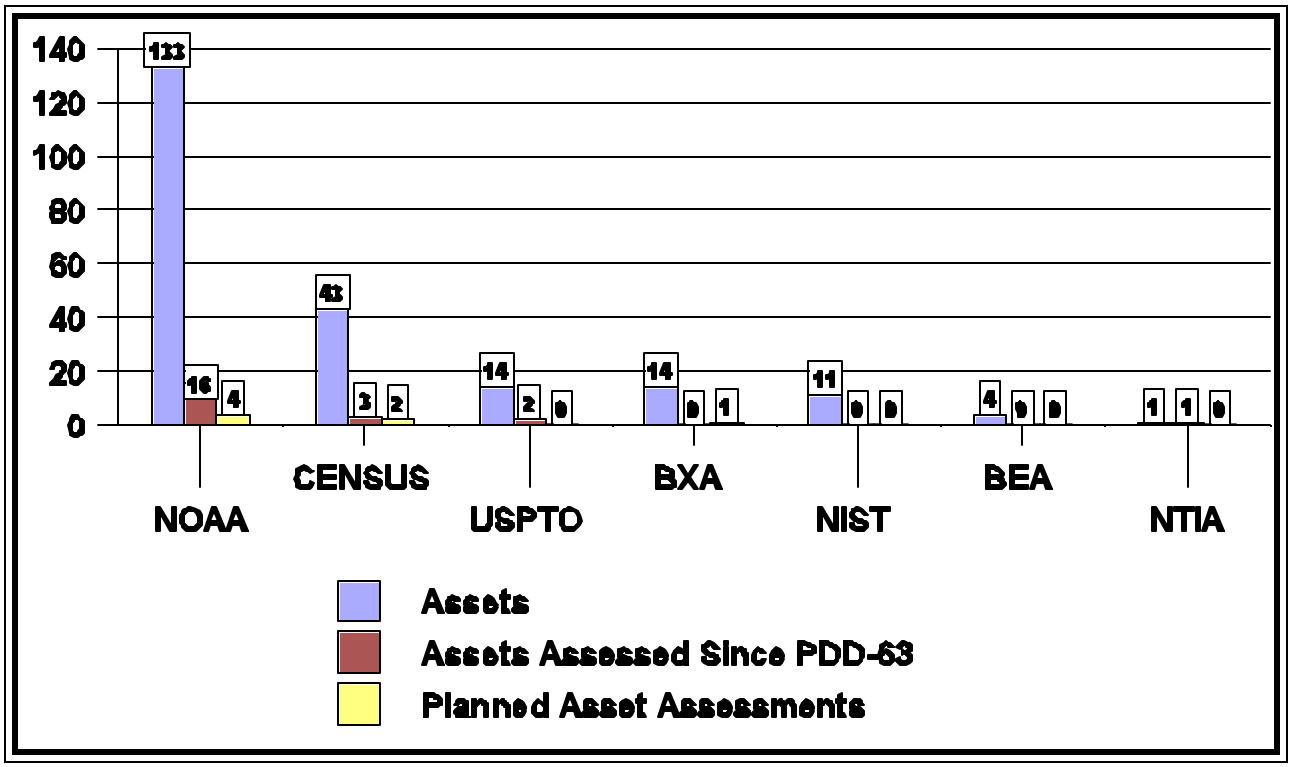
According to the Department's CIP plan, vulnerability assessments were to be completed by December 31, 1999, and remediation plans by February 29, 2000. These milestones were not met. The Department completed its MEI asset inventory and formulated a FY 2001 budget request in April 1999 for $79.2 million. The request included funding for IT system security plans, vulnerability assessments, corrective actions, training, and physical protection of assets. However, OMB rejected the request because the Department had not yet conducted vulnerability assessments and identified corrective actions and because it lacked accurate costs for corrective actions. Funding has been provided to the Department primarily for the national responsibilities of NIST, BXA, and NTIA as described in the introduction and appendixes to this report.

The National Plan requires that federal agencies conduct vulnerability assessments and then develop remediation plans. OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, refers to NIST's *An Introduction to Computer Security: The NIST Handbook* for guidance on effective assessments. According to the handbook, the framework for

[11] A "vulnerability assessment" is much more detailed than the "initial vulnerability assessment" defined in footnote 5. The *Department-Level Vulnerability Assessment*, published in April 1999, contains the Department's initial vulnerability assessment and includes an evaluation of all its assets for PDD-63 applicability so that priorities can be established for conducting more detailed vulnerability assessments of individual assets with the highest suspected risk.

[12] According to PDD-63, based upon vulnerability assessments, there will be a recommended remedial plan that identifies time lines for implementing corrective actions, responsibilities for implementation, and required funding.

Figure 2. Asset Assessment Status



computer security risk management includes identification of the asset risks followed by risk mitigation, which involves selecting and implementing security controls to reduce risk to a level acceptable to management. Remediation plans are a natural extension of vulnerability assessments and an agency's link to strategic IT planning and budget formulation.

NSA conducts vulnerability assessments for other federal agencies at their request as resources permit, at no cost to the agency. The Department requested NSA to conduct several vulnerability assessments. However, only two NOAA assessments and one Decennial Census assessment were completed.[13] Before NSA could perform additional assessments, it was inundated with priority requests for assessments of national security assets of the Department of Defense. Commerce resubmitted a request to NSA in February 2000 for nine additional assessments in priority order of PDD-63 criticality. NSA agreed only to evaluate BXA's Chemical Weapons Convention Information Management System, a classified system. USPTO vulnerability assessments were performed by various contractors. The assessments completed and scheduled will cover only 29, or about 12 percent, of the Department's 241 assets.

[13]A single vulnerability assessment may include one or more MEI assets.

In addition to having NSA perform vulnerability assessments, the Department had planned to contract for assessments for some of its largest and highest profile MEI assets. The FY 2001 budget request included $3.6 million for vulnerability assessments. It also planned to develop internal teams to perform assessments and develop remediation plans for a large number of additional assets. However, it has made little progress and does not have current milestones established for formulating the teams or conducting the assessments. Vulnerability assessment team meetings were held monthly from December 1998 through February 1999. At these meetings, operating units were asked to begin forming assessment teams that would be joined by departmental staff and contractors familiar with the vulnerability assessment process. However, no further action was taken, and no additional meetings have been held.

According to the National Plan, remediation plans are due with each annual budget request. But remediation plans cannot be prepared until vulnerability assessments are completed. The Department should develop remediation plans for the corrective actions needed as a result of vulnerability assessments already completed and prepare detailed justifications to support the FY 2002 budget formulation due this summer. Delays in preparing remediation plans already make it unlikely that the Department will meet the December 2000 goal of achieving an initial CIP operating capability.[14] Further delays in completing vulnerability assessments and remediation plans will make it difficult for the Department to meet the PDD-63 2003 implementation deadline.

B. CIP Budget Justifications Need to Be Completed from Remediation Plans

The Department faces a dilemma. It had planned to have a contractor perform additional vulnerability assessments with FY 2001 funds, but the funding was denied. Based on OMB's passback language for the internal FY 2001 CIP funding request, the Department needs to complete vulnerability assessments and develop accurate remediation costs to determine what level of funding is required for corrective actions. OMB also informed agencies at a March 8, 2000, CIAO conference that there likely will be no new funding added to the budget in FY 2002 specifically for internal CIP activities, as there was to fix year 2000 computer problems last year.

The National Plan states that the quality of CIP budget request data submitted by federal agencies did not meet OMB's typical expectations for several reasons. First, agency budget systems do not readily support the collection of CIP data. Until these systems are modified, collection of information on CIP programs and budgets will be manual and inexact. Second, the newness of CIP means that the government is still on the steep part of a learning curve. Third, individual agencies are still grappling

[14]The phrase "initial operating capability" is referred to in PDD-63 but it is not defined. The Department's definition is that (1) a broad level assessment of MEI should be completed, (2) remediation plans should be completed for assets considered to be the most at risk, and (3) fixes should be in place for the most vulnerable assets. We believe that the April 1999 *Department-Level Vulnerability Assessment* satisfies the first requirement, but the second and third requirements have not been met.

with the issue internally, and the interagency budget process for achieving consistency among agencies is still being defined. When OMB issued its first CIP budget data request last year, it sought information at an activity level. But because of inadequate activity descriptions and data presentation problems, it was unable to consolidate the data, making it difficult to perform meaningful cross-cutting reviews. OMB therefore lacked confidence in the data.

In preparation for the FY 2001 budget request, OMB, in conjunction with the National Coordinator, created a special process to review national and departmental requirements before the agencies and departments submitted their proposed budgets. The National Plan provides broad direction and guidance for agencies and departments. However, decisions about agency funding for CIP are being made in the regular OMB budget formulation process. Accordingly, agencies were asked to submit with their FY 2001 budget requests a remediation plan to justify funding. However, the cost estimates that the Department submitted did not contain the level of detail that OMB wanted and were not based on vulnerability assessments and remediation plans.

OMB approved only limited funding for a few agencies in the FY 2001 budget cycle. Agencies were informed by OMB at the CIAO conference that extremely detailed budget requests showing corrective actions are needed. This message also appears in written guidance from OMB Memorandum M-00-07, *Incorporating and Funding Security in Information Systems Investments*, dated February 28, 2000. The memorandum reminds agencies of OMB principles for incorporating and funding security as part of agency IT systems and architectures and of the decision criteria that will be used to evaluate security for information systems investments. The memorandum was written pursuant to the Clinger-Cohen Act, which directs OMB to develop, as part of the budget process, a mechanism to analyze, track, and evaluate the risks and results of major capital investments made by executive agencies for information systems. The criteria will be incorporated into future revisions of OMB Circular A-130 and, according to OMB, should be used in conjunction with Memorandum M-97-02, *Funding Information Systems Investment*, which also stresses the need for strong justifications accompanying budget requests.

C. Recommendation

We recommend that the Department's CIO:

3. Ensure that vulnerability assessments and remediation plans are completed by the dates established in the updated Departmental CIP plan and that improved CIP budget justifications are prepared. Emphasis should be placed on:

    a. Formulating, training, and coordinating Department of Commerce teams to conduct vulnerability assessments on priority assets based on a revised MEI asset inventory.

b. Expeditiously developing remediation plans for the MEI assets that already have been assessed for vulnerabilities and require corrective actions.

c. Developing remediation plans based on the results of future vulnerability assessments.

d. Working with the operating unit asset managers, acquisition offices, and budget offices in developing detailed budget justifications for CIP risk mitigation efforts and using the plans to formulate the FY 2002 budget.

D. CIO Response and OIG Comments

The CIO has scheduled training in September 2000 on NSA's infrastructure assessment methodology for the operating units, and will be encouraging the performance of self-assessments. Shortly, a notice will be sent to the operating units requiring the completion of corrective action plans for the assessments that have been completed, and corrective actions will be tracked in the IT Systems Data Base currently under development within the CIO's office. The CIO will also require that future assessments be followed by corrective action plans in a timely manner.

The CIO soon will send a notice to the operating units requiring the development of budget projections following the completion of corrective action plans for the assessments that have been completed. Several operating units have already brought FY 2002 budget requests before the Commerce IT Review Board for funding to perform vulnerability assessments and to implement corrective actions based on vulnerability assessments. The CIO's written response stated that because of constraints by OMB and the Department, CIP funding would not go forth in the FY 2002 budget. However, on August 11, 2000, the CIO informed the OIG that the Department has included three NOAA IT security/CIP budget initiatives in its FY 2002 budget request to OMB: High Performance Computing, Gateway Legacy System, and Network Security. These initiatives include several priority MEI assets that support weather forecasting.

The CIO's complete response is included as Appendix E.

Appendix A

NIST Candidate Research Areas Mandated by PDD-63

- Physical/cyber/human interfaces.
- Intrusion monitoring and response.
- Malicious code prevention and detection.
- Reconstitution.
- Characterizing infrastructures as end-to-end systems.
- Establishing information assurance as an engineering discipline, including development of engineering principles and metrics.
- Prototyping and testing end-to-end trustworthy systems.
- Robustness and resilience of highly complex nonlinear networks.
- Analysis of infrastructure interdependencies, including modeling, simulation, and database development.
- Other shortfalls such as public key infrastructure, testing, and security architectures.

Appendix B

2 Pages

National Plan Objectives and Programs to Implement PDD-63

To meet the ultimate goal established by PDD-63 of defending the nation's critical infrastructures against deliberate attack by 2003, the current version of the National Plan has been designed around three broad objectives:

- ***Prepare and Prevent***: The steps necessary to minimize the possibility of a significant and successful attack on our critical information networks, and to build an infrastructure that remains effective in the face of such attacks.

- ***Detect and Respond***: The actions required to identify and assess an attack in a timely way, and then to contain the attack, quickly recover from it, and reconstitute affected systems.

- ***Build Strong Foundations***: The things we must do as a nation to create and nourish the people, organizations, laws, and traditions that will make us better able to prepare and prevent, and detect and respond to attacks on our critical information networks.

The following 10 programs will achieve the objectives.

Prepare and Prevent

Program 1: Identify Critical Infrastructure Assets and Shared Interdependencies and Address Vulnerabilities.

Detect and Respond

Program 2: Detect Attacks and Unauthorized Intrusions.

Program 3: Develop Robust Intelligence and Law Enforcement Capabilities to Protect Critical Information Systems, Consistent with the Law.

Program 4: Share Attack Warnings and Information in a Timely Manner.

Program 5: Create Capabilities for Response, Reconstitution, and Recovery.

Build Strong Foundations

Program 6: Enhance Research and Development in Support of Programs 1-5.

Program 7: Train and Employ Adequate Numbers of Information Security Specialists.

Program 8: Conduct Outreach to Make Americans Aware of the Need for Improved Cyber - Security.

Program 9: Adopt Legislation and Appropriations in Support of Programs 1-8.

Program 10: In Every Step and Component of the Plan, Ensure the Full Protection of American Citizens' Civil Liberties, Their Rights to Privacy, and Their Rights to the Protection of Proprietary Data.

Appendix C

Model Role for the Inspector General Community in Critical Infrastructure Assurance

The Inspector General (IG) community will be proactively involved in the design and implementation of the federal government's critical infrastructure assurance program. To this end, emphasis will be placed on:

- Establishing the IG community as an integral part in the government's efforts to protect its critical infrastructure.
- Assessing agency compliance with PDD-63 and related infrastructure protection requirements and guidance, and ensuring consistency of application throughout the government.
- Reviewing agency infrastructure protection plans and vulnerability and risk assessments, as they are being developed and updated.
- Reviewing and commenting on proposed agency guidance, policies, and procedures related to protecting the government's critical infrastructure.
- Coordinating with the Critical Infrastructure Assurance Office and other national oversight organizations in reviewing applicable draft legislation and new and proposed regulations and policies that impact federal agencies and departments.
- Identifying factors that inhibit industry, and foreign, state, and local governments from effectively participating in the nation's infrastructure protection program.
- Identifying agency best practices and standards and assessing their potential for use in other agencies, and state and local governments.
- Identifying and using metrics to gauge government effectiveness in implementing infrastructure assurance.
- Making recommendations to the Administration, agency partners, and the Congress to enhance the effectiveness of the nation's critical infrastructure protection program.
- Serving as an independent check on management’s performance, not as a substitute for management’s responsibility, to ensure that protections (policies, procedures, and controls) are adequate and operating effectively.

Source: PCIE/ECIE.

Appendix D

Acronyms Used in This Report

BEA	Bureau of Economic Analysis
BXA	Bureau of Export Administration
CIAO	Critical Infrastructure Assurance Office
CICG	Critical Infrastructure Coordinating Group
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
ECIE	Executive Council on Integrity and Efficiency
ERT	Expert Review Team
FBI	Federal Bureau of Investigation
FY	fiscal year
GAO	General Accounting Office
IG	Inspector General
IT	information technology
MEI	Minimum Essential Infrastructure
NESDIS	National Environmental Satellite, Data, and Information Service
NIPC	National Infrastructure Protection Center
NIST	National Institute of Standards and Technology
NOAA	National Oceanic and Atmospheric Administration
NSA	National Security Agency
NTIA	National Telecommunications and Information Administration
OIG	Office of Inspector General
OMB	Office of Management and Budget
PCIE	President's Council on Integrity and Efficiency
PDD	Presidential Decision Directive
USPTO	United States Patent and Trademark Office

Appendix E

9 Pages

UNITED STATES DEPARTMENT OF COMMERCE
Chief Financial Officer
Assistant Secretary for Administration
Washington, D.C. 20230

AUG 7 2000

MEMORANDUM FOR Judith J. Gordon
Assistant Inspector General for Systems Evaluation

FROM for Roger W. Baker
Chief Information Officer

SUBJECT *Critical Infrastructure Protection: Early Strides Were Made, But Planning and Implementation Have Slowed*
Draft Inspection Report No. OSE-12680/June 2000

Thank you for your recently completed review of our Critical Infrastructure Protection (CIP) efforts to date. My staff found it a pleasure to work with yours in this cooperative effort. We found your staff to be professional and knowledgeable, and the results to be thorough, helpful, and enlightening. We look forward to working with you on related issues in the near future, and hope that this can be the beginning of a true partnership leading toward improving the security of Commerce's information technology resources.

Generally, we agree with your findings. Most of our comments do not reflect disagreement, but rather what we believe is the situation in which we find ourselves. That is, while we have believed in this program since its beginnings, our efforts have been slowed by a lack of funding for CIP. We must now direct our limited security resources to those areas that will be of most benefit to the Department of Commerce and in directions that we believe can be successful, that is, information technology security for mission critical systems (keeping CIP in mind).

The attached table addresses each finding and recommendation in detail. If you have any questions, please contact the Department's Information Technology Security Manager, Mr. Michael Lombard. He can be reached on (202) 482-0277, or by E-mail at mlombard@doc.gov.

Attachment

cc: Lisa Westerback
Mike Lombard
Karl Schornagel

Critical Infrastructure Protection: Early Strides Were Made, But Planning and Implementation Have Slowed
Draft Inspection Report No. OSE-12680/June 2000

Comments on Findings and Recommendations

August 7, 2000

OIG Finding or Recommendation	OCIO Comment
I. Department's Critical Infrastructure Protection Plan Needs to Be Revised	We agree that the Plan should be an accurate reflection of reality, should be adjusted to portray the current state of affairs, and should be kept up to date through the life of the program. In fact, we believe that the Plan was written for a very different approach than that which we feel would be successful today, and should be rewritten with our current understanding of the issues and environment. However, given the reluctance to fund CIP efforts, the workload of the IT Security Staff, and the critical need for IT security for Commerce mission critical systems, we feel that there are very limited resources to spend on rewriting the Plan at this time. When, and if, CIP receives funding priority, DoC will respond accordingly and dedicate appropriate resources to bringing the Plan to a current state of readiness. However, we do feel that there are some adjustments that would be beneficial now such as revising the asset list and target dates, strategic planning, evaluating new assets, and OIG notifications. We will endeavor to incorporate these changes in the near future.
A Elements of the Plan Are Outdated or Missing	We appreciate the perspective on the missing elements and will incorporate them in the major revision of the Plan.

B Important Milestones Have Slipped	We feel that the concept of concentrating on PDD-63 critical assets rather than those traditionally thought of as "mission critical" is easily misunderstood and is a hard sell to IT program managers. We feel that we are now coming to a better understanding of the issues and the scope of the problem and our planning has been adjusted accordingly. This will be reflected in future versions of the Plan. While we agree that new milestones can be set, we believe that these will be well beyond the time frames set in PDD-63, and will continue to be subject to change unless the political will can be generated to solve the funding problem.
C Recommendation:	
1. Include in the Department's updated CIP plan:	
a. A revised MEI asset list that prioritizes assets.	The asset list continues to be revised as we and the operating units come to a better understanding of CIP. The asset list will be kept up to date in future versions of the Plan.
b. The revised framework for conducting vulnerability assessments.	The original selection of the vulnerability assessment framework was based on its being the only choice at the time. It soon became apparent that it was unwieldy and would be impossible to implement. There are now several models for conducting vulnerability assessments that have been proposed for use in CIP. We are learning to use the model developed by NSA, and will possibly combine it with those published by the CIAO and NIST. As we settle on the methodology that works best for DoC, the revised framework will be described in the major revision of the Plan.

c.	Current budget estimates for CIP-related activities.	Current budget estimates for CIP-related activities will be included in the major revision of the Plan.
d.	A provision for evaluating new assets to determine whether they should be included as MEI.	A provision for evaluating new assets to determine whether they should be included as PDD-63 critical assets will be included in future versions of the Plan.
e.	A requirement to update vulnerability assessments.	A requirement to update vulnerability assessments will be included in future versions of the Plan.
f.	The development of a system for responding to significant infrastructure attacks in progress.	The development of a system for responding to significant infrastructure attacks in progress will be included in the major revision of the Plan.
g.	A requirement to notify OIG criminal investigators of infrastructure attacks.	The OCIO, OSY, and the OIG are working on a memorandum of agreement, which includes criminal investigators of infrastructure attacks. We need to understand the concerns of each office and resolve any conflicts. Appropriate notifications will be included in future versions of the Plan.
h.	A requirement that operating units incorporate security planning procedures into the basic design of new programs that include critical infrastructure.	A requirement that operating units incorporate security planning procedures into the basic design of new programs that include critical infrastructure will be included in future versions of the Plan.
i.	A provision for incorporating CIP functions into the Department's IT strategic planning and performance measurement frameworks.	While this function is currently being done, provisions for incorporating CIP functions into the Department's IT strategic planning and performance measurement frameworks will be included in future versions of the Plan.

	j. Updated milestones, including milestones for revising the MEI asset inventory and completing vulnerability assessments and remediation plans.	Updated milestones, including milestones for revising the PDD-63 critical asset inventory and completing vulnerability assessments and remediation plans will be included in future versions of the Plan.

II. Minimum Essential Infrastructure Asset Inventory Should Be Reevaluated	We agree that the asset inventory needs further revision and will take short term steps to refine the evaluation of those previously identified as most critical. However, given the reluctance to fund CIP efforts, the workload of the IT Security Staff, and the critical need for IT security for Commerce mission critical systems, we feel that there are very limited resources to spend on revising the entire inventory at this time. When, and if, CIP receives funding priority, DoC will respond accordingly and dedicate appropriate resources to bringing the CIP inventory current.
Recommendation	
2. Reevaluate the Department's Minimum Essential Infrastructure assets by the dates established in the updated Departmental CIP plan and include in the methodology:	
a. Increased involvement from operating units, including interviews with asset managers or others most knowledgeable about the asset's functions, dependencies, and end users.	We agree that involvement at the asset ownership level is critical to the success of this endeavor and our effort did involve CIOs and IT security officers from each operating unit in discussions about the process and about their assets in particular. Our work to identify lessons learned and with the CIAO to improve this process led to the formation of teams of executives, managers, and technical experts from each asset under review to participate in training, interviews, and evaluations. It is our intent to use this improved process in our next round of asset evaluations. However, it must be noted, that several operating units and line offices disagree with this approach and insist on the involvement of only one individual for the entire process for all assets in the OU/LO. We continue to work to correct what we believe is a misunderstanding of the process and resulting reduced output quality.

	b. Improved guidance to operating personnel involved in assessments.	We agree that the guidance could be improved for the execution of the initial assessment and have taken an active part in identifying this issue and in revising the methodology as it is currently being used by the CIAO. We will keep current as the methodology is implemented and improve our process accordingly.

III. Vulnerability Assessments, Remediation Plans, and Budget Justifications Need to Be Completed	
A Vulnerability Assessments and Remediation Plans Need to Be Developed	We agree. Several operating units have brought FY 2002 budget requests before the Commerce IT Review Board (CITRB) for the funding to perform vulnerability assessments.
B CIP Budget Justifications Need to Be Developed from Remediation Plans	We agree. Several operating units have brought FY 2002 budget requests before the CITRB for the funding to perform corrective actions based on vulnerability assessments.
C Recommendation	
3. Ensure that vulnerability assessments and remediation plans are completed by the dates established in the updated Departmental CIP plan and that improved CIP budget justifications are prepared. Emphasis should be placed on:	
a. Formulating, training, and coordinating Department of Commerce teams to conduct vulnerability assessments on priority assets based on a revised MEI asset inventory.	We have scheduled training in September 2000, on the NSA Infrastructure Assessment Methodology for the operating units, and will be encouraging the performance of self assessments.
b. Expeditiously developing remediation plans for the MEI assets that already have been assessed for vulnerabilities and require corrective actions.	We will shortly be sending a notice to the operating units requiring the completion of corrective action plans for the assessments that have been completed. Corrective actions will be tracked in the IT Systems Data Base currently under development in the OS/OCIO/OIPPR.

c.	Developing remediation plans based on the results of future vulnerability assessments.	We will require that future assessments be followed by corrective action plans in a timely manner.
d.	Working with the operating unit asset managers, acquisition offices, and budget offices in developing detailed budget justifications for CIP risk mitigation efforts and using the plans to formulate the FY 2002 budget.	We will shortly be sending a notice to the operating units requiring the development of budget projections following the completion of corrective action plans for the assessments that have been completed. However, it must be noted that we are under constraints by OMB and the DoC Budget Office to limit FY 2002 budget requests to current services, with anomalies. CIP is not considered by the Budget Office as current services, nor do we expect that it will be seen as an anomaly.