using encryption software. Paper records, when created, are kept in file folders and cabinets in secure rooms.

RETRIEVABILITY:

Records are retrieved by name, Social Security Number, or Applicant or Employee ID.

SAFEGUARDS:

Computer records are protected by a password system. Paper output is stored in locked metal containers or in secured rooms when not in use. Information is released to authorized officials based on their need to know.

RETENTION AND DISPOSAL:

Records are disposed of by shredding or burning as scheduled in the handbook, GSA Records Maintenance and Disposition System (OAD P 1820.2).

SYSTEM MANAGER AND ADDRESS:

CHRIS Program Manager (CID), Office of the Chief Information Officer, Office of the Chief Human Capital Officer, General Services Administration, 1800 F Street, NW., Washington, DC 20405.

NOTIFICATION PROCEDURE:

Address inquiries to: Director of Human Resources Services (CP), Office of the Chief People Officer, General Services Administration, 1800 F Street, NW., Washington, DC 20405; or, for regional personnel records, to the regional Human Resources Officer at the addresses listed above under System Location.

RECORD ACCESS PROCEDURES:

Requests from individuals for access to their records should be addressed to the system manager.

CONTESTING RECORD PROCEDURES:

Rules for contesting the content of a record and appealing a decision are contained in 41 CFR 105–64.

RECORD SOURCE CATEGORIES:

The sources for the system information are the individuals themselves, other employees, supervisors, management officials, officials of other agencies, and record systems GSA/HRO–37, OPM/GOVT–1, and EEOC/GOVT–1.

[FR Doc. E8–11822 Filed 5–30–08; 8:45 am]

BILLING CODE 6820–34–M

GOVERNMENT ACCOUNTABILITY OFFICE

Appointments to the Medicare Payment Advisory Commission

AGENCY: Government Accountability Office (GAO).

ACTION: Notice of appointments.

SUMMARY: The Balanced Budget Act of 1997 established the Medicare Payment Advisory Commission (MedPAC) and gave the Comptroller General responsibility for appointing its members. This notice announces three new appointments and two reappointments to fill the vacancies occurring this year.

DATES: Appointments are effective May 1, 2008 through April 30, 2011, except as noted.

ADDRESSES: GAO: 441 G Street, NW., Washington, DC 20548.

MedPAC: 601 New Jersey Avenue, NW., Suite 9000, Washington, DC 20001.

FOR MORE INFORMATION CONTACT: GAO: Office of Public Affairs, (202) 512–4800.

MedPAC: Mark E. Miller, Ph.D., (202) 220–3700.

SUPPLEMENTARY INFORMATION: To fill this year's vacancies I am announcing the following:

Newly appointed members are Peter W. Butler, M.H.S.A., Executive Vice President and Chief Operating Officer, Rush University Medical Center; Michael Chernew, Ph.D., professor, Department of Health Care Policy; and George N. Miller, Jr., M.H.S.A., Regional President and Chief Executive Officer, Community Mercy Health Partners.

Reappointed members are Jennie Chin Hansen, R.N., M.S.N., member, Board of Directors, AARP; and Nancy M. Kane, D.B.A., professor of management, Department of Health Policy Management, Harvard School of Public Health.

(Sec. 4022, Pub. L. 105–33, 111 Stat. 251, 350)

Gene L. Dodaro,

Acting Comptroller General of the United States.

[FR Doc. E8–12023 Filed 5–30–08; 8:45 am]

BILLING CODE 1610–02–M

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of the Secretary

Office of Resources and Technology; Statement of Organization, Functions and Delegations of Authority

Part A, Office of the Secretary, Statement of Organization, Functions and Delegations of Authority for the Department of Health and Human Services (HHS) is being amended at Chapter AM, Office of Resources and Technology, as last amended at 72 FR 2282–88 on January 18, 2007, and more recently at 72 FR 56074, on October 2, 2007. This reorganization is to establish within the Office of the Chief Information Officer (AMM), a new Office of Information Technology Security (AMM6). The changes are as follows:

I. Under Chapter AM, Section AMM. 10 Organization, delete in its entirety and replace with the following:

AMM.10 Organization. The Office of the Chief Information Officer (OCIO) is headed by the Deputy Assistant Secretary for Information Technology/HHS Chief Information Officer (CIO), who reports to the Secretary and the Assistant Secretary for Resources and Technology (ASRT). The HHS CIO serves as the primary IT leader for the Department, and the OCIO consists of the following:

- Immediate Office (AMM).
- Office of Resources Management (AMM2).
- Office of Enterprise Architecture (AMM4).
- Office of Enterprise Project Management (AMM5).
- Office of Information Technology Security (AMM6).

II. Under AM, Section AMM.20 Functions, make the following changes:

A. Under Paragraph 3, ''Office of Enterprise Architecture (AMM4),'' delete in its entirety and replace with the following:

3. *Office of Enterprise Architecture (AMM4):* The Office of Enterprise Architecture (OEA) is headed by the Director, Office of Enterprise Architecture who is also the HHS Chief Enterprise Architect and supports all planning and enterprise programs that fall under the OCIO.

The OEA is responsible for:

a. Working with OPDIV Chief Information Officers (CIOs) to support Government-wide initiatives of the Federal CIO Council and to identify opportunities for participation and consultation in information technology projects with major effects on OPDIV program performance.

b. Providing leadership in the planning, design, and evaluation of major Departmental projects and oversight throughout project rollout and perform post implementation performance assessments.

c. Assessing risks that major information systems pose to performance of program operations and administrative business throughout the Department, develops risk assessment policies and standard operating procedures and tools, and uses program outcome measures to gauge the quality of Departmental information resources management.

d. Coordinating the Department's strategic planning, capital planning and investment control (CPIC), budgeting and performance management processes for information technology, and provides direct planning development and support to assure that IRM plans support agency business planning and mission accomplishment.

e. Coordinating the activities of the Departmental Information Technology Investment Review Board (ITIRB) in assessing and prioritizing the Department's major information systems, and in analyzing and evaluating IT investment decisions. Reviews OPDJV ITIRB implementations, IT capital funding decisions, and use of performance metrics to evaluate programs for both initial and continued funding.

f. Coordinating and supporting the Department's Chief Information Officer's Council, whose membership consists of the Chief Information Officers from each OPDIV.

g. Representing the Department through participation on interagency and Departmental work groups and task forces, as appropriate.

h. Working with OPDIV Chief Information Officers to identify opportunities for administering information management functions and telecommunications initiatives with major effects on OPDIV performance. OEA provides leadership primarily in defining alternatives for acquisition of telecommunications services and coordinating implementation of information management initiatives in conjunction with the Director of the Office of Enterprise Project Management and the HFJS Chief Enterprise Architect.

i. Providing support for special priority initiatives identified by the CIO.

B. Add the following new paragraph at the end of Section AMM.20 Functions, ''Office of the Chief Information Officer (AMM6).''

5. *Office of Information Technology Security (AMM6).* The Office of Information Technology Security (OITS) is headed by the Director, (OITS), who is also HHS Chief Information Security Officer (CISO), which manages HHS Security Program. The Office provides management leadership in IT security policy and guidance, expert advice and collaboration among the Operating Divisions (OPDIVs) and the Staff Divisions (STAFFDIVs) in developing, promoting and maintaining IT security measures to adequately and cost effectively protect and ensure the confidentiality, integrity and timely availability of all data and information in the custody of the Department as well as of the information systems required to meet the Department's current and future business needs. OJTS is responsible for:

a. Developing, implementing and administering the program to protect the information resources of the Department. This includes management and oversight of activities under the Federal Information Security Management Act (FISMA), IT critical infrastructure protection (CIP), and Department-wide security contracts and high level project management of OPDIV security programs, such as corrective action plans and security policies.

b. Implementing and administering the HHS security program to protect the information resources of the Department in compliance with legislation, Executive Orders, directives of the Office of Management and Budget (OMB), or other mandated requirements (e.g., the Clinger Cohen Act, Presidential Decision Directive 63, and OMB Circular A–130), the National Security Agency, and other Federal agencies.

c. Directing the development of and implementing cyber security policies and guidance for the Department, including requirements for employees and contractors who are responsible for systems of data, or for the acquisition, management, or use of information resources.

d. Monitoring information system security program activities in the Department by reviewing OPDIVs and STAFFDFVs security plans for sensitive systems, recommending improvements, and evaluating safeguards to protect major information systems, or IT infrastructure.

e. Responding to requests in conjunction with 0MB Circular A–130, the Computer Security Act of 1987, and Presidential Decision Directive 63, or other legislative or mandated requirements related to IT security or privacy.

f. Monitoring all Departmental systems development and operations for security and privacy compliance and providing advice and guidance to ensure compliance standards are included throughout system life cycle development.

g. Reviewing Departmental ITIRB and ClO Council business cases (as well as 0MB circular A–11 requirements) for assurance of security and privacy compliance.

h. Recommending to the ClO to grant or deny programs the authority to operate information systems, based on security compliance.

i. Establishing and leading Department-wide teams to conduct reviews to protect HHS cyber and personnel security programs and conduct vulnerability assessments of HHS critical assets. This includes regular certification of existing systems as well as newly implemented systems. The OITS activities involving personnel and cyber security are coordinated and synchronized with the Office of Security and Strategic Information.

j. Reviewing the Department's information resources for fraud, waste, and abuse to avoid having redundant resources, in conformance with the Clinger-Cohen Act.

k. Developing, implementing, and evaluating employee cyber security awareness and training program to meet the requirements as mandated by 0MB Circular A–130 and the Computer Security Act.

l. Establishing and providing leadership to the Subcommittee of the HHS ClO Council on Security.

m. Establishing and leading the HHS Computer Security Incident Response Capability team, the Department's overall cyber security incident response/coordination center and primary point of contact for Federal Computer Incident Response Capability (FedCIRC) and National Infrastructure Protection Center (NIPC).

IV. Continuation of Policy: Except as inconsistent with this reorganization, all statements of policy and interpretations with respect to the Office of Infonnation and Resources Management heretofore issued and in effect prior to this reorganization are continued in full force and effect with respect to the Office of the Chief Information Officer.

V. Delegation of Authority: All delegations and redelegations of authority previously made to officials and employees of the Office of the Chief Information Officer will continue in them or their successors pending further redelegation, provided they are consistent with this reorganization.

VI. Funds, Personnel, and Equipment: Transfer of organizations and functions affected by this reorganization shall he accompanied by direct and support funds, positions, personnel, records, equipment, supplies, and other sources.

Dated: May 19, 2008.

Joe W. Ellis,

Assistant Secretary for Administration and Management.

[FR Doc. E8–12025 Filed 5–30–08; 8:45 am]

BILLING CODE 4150–22–M