information systems to access organizational information systems and information that are intended for public access (e.g., individuals accessing federal information through public interfaces to organizational information systems).

ii. Establish terms and conditions for the use of external information systems in accordance with organizational security policies and procedures. The terms and conditions should address, at a minmum: (A) the types of applications that can be accessed on the organizational information system from the external information system; and (B) the maximum Federal Information Processing Standard 199 security category of information that can be processed, stored, and transmitted on the external information system.

iii. Prohibit authorized individuals from using an external information system to access the information system or to process, store, or transmit organization-controlled information except in situations where the organization: (A) Can verify the employment of required security controls on the external system as specified in the organization's information security policy and system security plan; or (B) has approved information system connection or processing agreements with the organizational entity hosting the external information system.

IV. Privacy

Agencies should review the OMB memorandum entitled ''Safeguarding Personally Identifiable Information,'' dated May 22, 2006, and ensure that their respective telework technology infrastructures, practices and procedures are in compliance with that memorandum and the Privacy Act. The OMB memorandum reemphasizes the many responsibilities under law and policy to safeguard sensitive personally identifiable information appropriately. Among other things, the Privacy Act requires each agency to establish:

''Rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of [the Privacy Act], including any other rules and procedures adopted pursuant to [the Privacy Act] and the penalties for noncompliance;'' [and]

''appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.'' (5 U.S.C. 552a(e)(9)–(10))

V. Training

Teleworkers should receive adequate training on the use of IT systems and applications needed for effective job performance. This should include any specialized training associated with (1) effective use of remote access and other resources needed for working remotely, and (2) security awareness and responsibility. In addition, agencies are encouraged to provide opportunities for teleworkers to practice in a telework situation.

VI. Technical Support

a. Agencies should (1) provide adequate and effective Help Desk support for teleworkers, and (2) require Help Desk personnel to possess the skills, procedures, and resources needed for resolving teleworker issues, such as remote access hardware and software issues.

b. Where feasible and applicable, agencies should provide routine systems maintenance via remote transmission procedures such as transmitting (''pushing'') software and system upgrades out to the teleworker's alternative worksite as opposed to requiring the teleworker to bring a computer to the agency worksite for maintenance.

VII. Additional References and Resources

a. Office of Management and Budget (see *http://www.whitehouse.gov/omb/memoranda/m03-18.pdf*).

b. Government Accountability Office (see *http://www.gao.gov*).

VIII. Commonly Asked Questions

a. May an employee use his or her own personal computer equipment to conduct official business from an alternative worksite? If so, who is responsible for maintaining an employee's personally-owned equipment that is used for official business?

Yes, provided certain conditions are met, agencies may permit employees to use personally-owned equipment to conduct official business. If an agency permits the use of personally owned equipment, the employee must agree to allow the agency to (1) configure that equipment with the proper hardware and software necessary for secure and effective job performance, and (2) access the equipment, as needed, to verify compliance with agency policy and procedures. Additional conditions that must be met are set forth in NIST Special Publication 800–53, Rev. 1, on page 64, as follows:

''The organization prohibits authorized individuals from using an external information system to access the information system or to process, store, or transmit organization-controlled information except in situations where the organization: (i) Can verify the employment of required security controls on the external system as specified in the organization's information security policy and system security plan; or (ii) has approved information system connection or processing agreements with the organizational entity hosting the external information system.''

If the agency allows the use of personally-owned equipment for official business, then the telework agreement should clearly identify the employee's and agency's obligations for appropriate operation, repair, and maintenance of the equipment. While agencies are responsible for Government-owned equipment regardless of location, they are not required to be responsible for employee-owned equipment. At their sole discretion, however, agencies may assume responsibility for employee-owned equipment that is used to conduct official business. For example, agencies may authorize Help Desks or other agency personnel or resources to (1) fix a problem with the employee's personally-owned equipment, (2) help the employee fix the problem, or (3) provide, install, and/or upgrade Government-owned software on employee-owned equipment. If an agency permits the use of personally-owned equipment, the employee must agree to allow the agency to configure that equipment with the proper hardware and software including security, communications and applications.

b. Are there policies for ''limited personal use'' of Government e-mail and internet systems?

Yes. The Office of Management and Budget expects all agencies to establish personal use policies consistent with the recommended guidance developed by the CIO Council in 1999 (see ''Personal Use Policies and 'File Sharing' Technology'' memorandum at: *http://www.whitehouse.gov/omb/memoranda/fy04/m04-26.html*). In addition, NIST Special Publication 800–53, Rev. 1, under the section titled Supervision and Review—Access Control, recommends that agencies supervise and review the activities of users with respect to the enforcement and usage of information system access controls. According to this guidance, agencies should review audit records (e.g., user activity logs) for inappropriate activities in accordance with organizational procedures and investigate unusual information system-related activities.

c. Are there any other Guidelines for Alternative Workplace Arrangements?

Yes. For additional guidance, see FMR Bulletin, 2006–B3, Guidelines for Alternative Workplace Arrangements, Sections I through XV, dated March 17, 2006.

[FR Doc. 07–951 Filed 3–1–07; 8:45 am]

BILLING CODE 6820–RH–M

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of the Secretary

Notice of Meeting: Secretary's Advisory Committee on Genetics, Health, and Society

Pursuant to Public Law 92–463, notice is hereby given of the twelfth meeting of the Secretary's Advisory Committee on Genetics, Health, and Society (SACGHS), U.S. Public Health Service. The meeting will be held from 8 a.m. to approximately 5 p.m. on Monday, March 26, 2007 and 8 a.m. to approximately 5 p.m. on Tuesday, March 27, 2007, at the Marriott Inn and Conference Center, University of Maryland—College Park, 3501 University Boulevard East, Adelphi, MD 20783. The meeting will be open to the public with attendance limited to space available. The meeting also will be Web cast.

The agenda will focus on the oversight of genetic testing, including the role of the private sector in assuring the quality and validity of genetic tests; the impact of gene patents and licensing practices on patient access to genetic technologies, including a progress report on the Committee's study; and the status of Federal genetic information nondiscrimination legislation. The Committee will be briefed on the Secretary's Personalized Health Care Initiative and the work of the American Health Information Community, particularly its Personalized Health Care Working Group. The Committee's report on the Policy Issues Associated with Undertaking a New Large U.S. Population Cohort Project on Genes, Environment and Disease will be released at the meeting. There also will be updates on the Committee's draft report on pharmacogenomics and several Federal initiatives and activities.

Time will be provided each day for public comments. The Committee would welcome hearing from anyone wishing to provide public comment on any issue related to genetics, health and society. Individuals who would like to provide public comment should notify the SACGHS Executive Secretary, Ms. Sarah Carr, by telephone at 301–496–9838 or e-mail at *sc112c@nih.gov.* The SACGHS office is located at 6705 Rockledge Drive, Suite 750, Bethesda, MD 20892. Anyone planning to attend the meeting, who is in need of special assistance, such as sign language interpretation or other reasonable accommodations, is also asked to contact the Executive Secretary.

Under authority of 42 U.S.C. 217a, Section 222 of the Public Health Service Act, as amended, the Department of Health and Human Services established SACGHS to serve as a public forum for deliberations on the broad range of human health and societal issues raised by the development and use of genetic and genomic technologies and, as warranted, to provide advice on these issues. The draft meeting agenda and other information about SACGHS, including information about access to the Web cast, will be available at the following Web site: *http://www4.od.nih.gov/oba/sacghs.htm.*

Dated: February 22, 2007.

Anna Snouffer,

Acting Director, NIH Office of Federal Advisory Committee Policy.

[FR Doc. 07–973 Filed 3–1–07; 8:45 am]

BILLING CODE 4140–01–M

DEPARTMENT OF HEALTH AND HUMAN SERVICES

National Institute for Occupational Safety and Health; Designation of a Class of Employees for Addition to the Special Exposure Cohort

AGENCY: National Institute for Occupational Safety and Health (NIOSH), Department of Health and Human Services (HHS).

ACTION: Notice.

SUMMARY: The Department of Health and Human Services (HHS) gives notice of a decision to designate a class of employees at General Atomics in La Jolla, California, as an addition to the Special Exposure Cohort (SEC) under the Energy Employees Occupational Illness Compensation Program Act of 2000. On February 16, 2007, the Secretary of HHS designated the following class of employees as an addition to the SEC:

Atomic Weapons Employer (AWE) employees who were monitored or should have been monitored for exposure to ionizing radiation while working at the General Atomics facility in La Jolla, California at the following locations: Science Laboratories A, B, and C (Building 2); Experimental Building (Building 9); Maintenance (Building 10); Service Building (Building 11); Buildings 21 and 22; Hot Cell Facility (Building 23); Waste Yard (Buildings 25 and 26); Experimental Area (Buildings 27 and 27–1); LINAC Complex (Building 30); HTGR–TCF (Building 31); Fusion Building (Building 33); Fusion Doublet III (Building 34); SV–A (Building 37); SV–B (Building 39); and SV–D (no building number) for a number of work days aggregating at least 250 work days from January 1, 1960, through December 31, 1969, or in combination with work days within the parameters established for one or more other classes of employees in the Special Exposure Cohort.

This designation will become effective on March 18, 2007, unless Congress provides otherwise prior to the effective date. After this effective date, HHS will publish a notice in the **Federal Register** reporting the addition of this class to the SEC or the result of any provision by Congress regarding the decision by HHS to add the class to the SEC.

FOR FURTHER INFORMATION CONTACT: Larry Elliott, Director, Office of Compensation Analysis and Support, National Institute for Occupational Safety and Health (NIOSH), 4676 Columbia Parkway, MS C–46, Cincinnati, OH 45226, Telephone 513–533–6800 (this is not a toll-free number). Information requests can also be submitted by e-mail to *OCAS@CDC.GOV.*

Dated: February 23, 2007.

John Howard,

Director, National Institute for Occupational Safety and Health.

[FR Doc. 07–948 Filed 3–1–07; 8:45 am]

BILLING CODE 4160–17–M

DEPARTMENT OF HEALTH AND HUMAN SERVICES

National Institute for Occupational Safety and Health; Designation of a Class of Employees for Addition to the Special Exposure Cohort

AGENCY: National Institute for Occupational Safety and Health (NIOSH), Department of Health and Human Services (HHS).

ACTION: Notice.

SUMMARY: The Department of Health and Human Services (HHS) gives notice of a decision to designate a class of employees at the Monsanto Chemical Company in Dayton, Ohio, as an addition to the Special Exposure Cohort (SEC) under the Energy Employees Occupational Illness Compensation Program Act of 2000. On February 16, 2007, the Secretary of HHS designated the following class of employees as an addition to the SEC:

Atomic Weapons Employer (AWE) employees who were monitored or should have been monitored for exposure to ionizing radiation while working at Monsanto Chemical Company Units I, III, or IV in Dayton, Ohio, for a number of work days aggregating at least 250 work days during the period from January 1, 1943, through December 31, 1949, or in combination with work days within the parameters established for one or more other classes of employees in the Special Exposure Cohort.

This designation will become effective on March 18, 2007, unless Congress provides otherwise prior to the effective date. After this effective date, HHS will publish a notice in the **Federal Register** reporting the addition of this class to the SEC or the result of any provision by Congress regarding the decision by HHS to add the class to the SEC.

FOR FURTHER INFORMATION CONTACT: Larry Elliott, Director, Office of Compensation Analysis and Support, National Institute for Occupational Safety and Health (NIOSH), 4676 Columbia Parkway, MS C–46, Cincinnati, OH 45226, Telephone 513–533–6800 (this is not a toll-free number). Information requests can also be submitted by e-mail to *OCAS@CDC.GOV.*