B. Procedures

Per diem rates are published on the Internet at *www.gsa.gov/perdiem* as an FTR Per Diem Bulletin and published in the **Federal Register** on a periodic basis. This process ensures timely increases or decreases in per diem rates established by GSA for Federal employees on official travel within CONUS. Notices published periodically in the **Federal Register**, such as this one, now constitute the only notification of revisions in CONUS per diem rates to agencies.

Dated: December 22, 2004.

Becky Rhodes,

Deputy Associate Administrator. Office of Transportation and Personal Property.

[FR Doc. 04–28494 Filed 12–28–04; 8:45 am]

BILLING CODE 6820–14–S

GENERAL SERVICES ADMINISTRATION

Public Meeting Addressing Privacy and Policy Issues in a Common Identification Standard for Federal Employees and Contractors

AGENCY: Office of Electronic Government and Technology, GSA.

ACTION: Notice of public meeting.

SUMMARY: The General Services Administration, in partnership with the Department of Commerce and the Office of Management and Budget will host a public meeting to seek individual views on the policy, privacy, and security issues associated with the Common Identification Standard for Federal Employees and Contractors as outlined in Homeland Security Presidential Directive 12 (HSPD–12). The public meeting is on the draft common identification standard (Federal Information Processing Standard 201) and will inform future HSPD–12 implementation guidance issued by the Office of Management and Budget.

DATES: The public meeting is on January 19, 2005, from 8:30 a.m. to noon at the Auditorium of the Potomac Center Plaza, 550 12th Street, SW., Washington, DC 20202, near the Smithsonian and L'Enfant Plaza Metro Stations. The meeting is open to the public and there is no fee for attendance. All attendees must pre-register and present government-issued photo identification to enter the building. Students may present their student ID.

Registration: Please e-mail your plan to attend to Sara Caswell, *sara@nist.gov*. Sara can be reached at 301–975-4634 if you have questions regarding registration. Registration information must be received by 5 p.m. e.s.t., January 11, 2005.

Requests To Speak at the Meeting: Written requests to speak at the meeting are required before January 5, 2005, and should be sent via e-mail to *eauth@omb.eop.gov* or by fax to 202–395–5167. In their requests, individuals should include a statement describing their expertise in, or knowledge of, the issues on which the public meeting will focus. Potential speakers should provide their contact information, including a telephone number, facsimile number, and e-mail address, to enable notification if selected. Selected speakers will be notified on or before Friday, January 7, 2005. There will be open microphone time during the last half hour of the meeting.

FOR FURTHER INFORMATION CONTACT: Ms. Jeanette Thornton, (202) 395–3562 or Ms. Judith Spencer, (202) 208–6576. An agenda and additional information for attendees will be posted on the *www.csrc.nist.gov/piv-project* Web site prior to the meeting.

SUPPLEMENTARY INFORMATION: On August 27, 2004, the President issued HSPD–12 Common Identification Standard for Federal Employees and Contractors.

As the Directive explained, ''wide variations in the quality and security of forms of identification used to gain access to secure Federal and other facilities where there is potential for terrorist attacks need to be eliminated. Therefore, it is the policy of the United States to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees).

''Secure and reliable forms of identification for purposes of this directive means identification that (a) is issued based on sound criteria for verifying an individual employee's identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established by an official accreditation process. The Standard will include graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application. The Standard shall not apply to identification associated with national security systems as defined by 44 U.S.C. 3542(b)(2).''

HSPD–12 directed the Secretary of Commerce to ''promulgate in accordance with applicable law a Federal standard for secure and reliable forms of identification (the ''Standard'') not later than 6 months after the date of this directive in consultation with the Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the Director of the Office of Management and Budget (OMB), and the Director of the Office of Science and Technology Policy.''

On November 8, 2004, NIST published a draft standard. The Standard and supporting documents are available at *http://csrc.nist.gov/piv-project*. The standard was open for public comment until December 23, 2004. On February 27, 2005 the standard will be promulgated. Information on the past two public workshops on the standard is available at *www.csrc.nist.gov/piv-project*.

The public meeting to address ''Privacy and Security Issues in a Common Identification Standard for Federal Employees and Contractors'' will focus on the specific issues raised in HSPD–12. Meeting speakers should address the privacy and security concerns as they may affect individuals, including Federal employees and contractors as well as the public at large, in implementation.

By bringing together card and biometric experts, privacy advocates, academics, and other interested parties, the public meeting will present views on how to develop policies to implement the Standard without compromising users' privacy and security.

The session will include introductory remarks and speakers to discuss key questions, such as:

1. How do the proposed technologies in the draft FIPS 201 standard affect privacy and security?

- Does the proposed use of contact and contactless smart card chips raise privacy or security concerns?
- Do the biometric (fingerprint and facial image) standards as proposed, raise privacy or security concerns?
- Does the assignment of a permanent or persistent employee identification number raise privacy concerns?
- Do other applications or features of the card, as proposed raise concerns?

2. Do the proposed credential issuance policies and procedures raise privacy and security concerns?

3. What federal uses of the identification raise privacy and security concerns?

4. Are there means to address privacy and security in the development of the card standard and implementation guidance?

• Can privacy enhancing technologies be built into the card?

• How can we limit non-federal uses of the card?

• What training do employees and contractors need to properly secure their cards?

• What training should card issuers have? Security personnel?

• What law and policies must agencies consider in planning for and implementing the new cards?

Dated: December 22, 2004.

G. Martin Wagner,

Associate Administrator for Governmentwide Policy.

[FR Doc. 04–28493 Filed 12–28–04; 8:45 am]

BILLING CODE 6820–WY–P

GENERAL SERVICES ADMINISTRATION

Privacy Act of 1974; Proposed New Privacy Act System of Records

AGENCY: General Services Administration

ACTION: Notice of proposed new Privacy Act system of records

SUMMARY: The General Services Administration (GSA) proposes to establish a new system of records titled ''Internal Evaluation Case Files,'' (GSA/ADM–25). The system of records, to be maintained by GSA's Office of Inspector General (OIG), is being established to create a record keeping system containing evaluations and investigations of OIG personnel. The records in the system currently are a part of another OIG system of records, Investigation Case Files (GSA/ADM–24). The OIG has determined that a separate system would enhance the OIG's ability to conduct internal investigations.

DATES: The system of records will become effective without further notice on January 28, 2005 unless comments received on or before that date result in a contrary determination.

ADDRESSES: Comments should be submitted to the Office of Counsel to the Inspector General (JC), Office of Inspector General, General Services Administration, 1800 F Street NW, Washington DC 20405.

FOR FURTHER INFORMATION CONTACT: GSA Privacy Act Officer, General Services Administration, Office of the Chief People Officer, 1800 F Street NW, Washington DC 20405; telephone (202) 501–1452.

Dated: November 19, 2004

June V. Huber,

Director, Office of Information ManagementOffice of the Chief People Officer

GSA/ADM–25

System name: Internal Evaluation Case Files.

System location: This system is located in the GSA Office of Inspector General, 1800 F Street, NW, Washington, DC 20405. The database for this system is on a local area network in the GS Building and is operated by the System Development and Support Division of the Office of Inspector General.

Categories of individuals covered by the system: Individuals covered by the system are employees and former employees of the GSA Office of Inspector General. The system also includes any person who was the source of a complaint or allegation; a witness who has information or evidence on any aspect of an investigation; and any possible or actual suspect in a civil, criminal, or administrative action.

Categories of records in the system: Investigative files containing information such as name, date and place of birth, experience, and investigative material that is used as a basis for taking civil, criminal, and administrative actions.

Authority for maintenance of the system: 5 U.S.C. App. 3., Section 2 *et seq.*

Purpose: The system serves as a basis for issuing subpoenas and taking civil, criminal, and administrative actions.

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

Records are used by GSA officials and representatives of other Government agencies on a need–to–know basis in the performance of their official duties under the authorities set forth above and for the following routine uses.

1. A record of any case in which there is an indication of a violation of law, whether civil, criminal, or regulatory in nature, may be disseminated to the appropriate Federal, State, local, or foreign agency charged with the responsibility for investigating or prosecuting such a violation or charged with enforcing or implementing the law.

2. A record may be disclosed to a Federal, State, local, or foreign agency or to an individual organization in the course of investigating a potential or actual violation of any law, whether civil, criminal, or regulatory in nature, or during the course of a trial or hearing or the preparing for a trial or hearing for such a violation, if there is reason to believe that such agency, individual, or organization possesses information relating to the investigation, and disclosing the information is reasonably necessary to elicit such information or to obtain the cooperation of a witness or an informant.

3. A record relating to a case or matter may be disclosed in an appropriate Federal, State, local, or foreign court or grand jury proceeding in accordance with established constitutional, substantive, or procedural law or practice, even when the agency is not a party to the litigation.

4. A record relating to a case or matter may be disclosed to an actual or potential party or to his or her attorney for the purpose of negotiation or discussion on matters such as settlement of the case or matter, plea–bargaining, or informal discovery proceedings.

5. A record relating to a case or matter that has been referred by an agency for investigation, prosecution, or enforcement or that involves a case or matter within the jurisdiction of any agency may be disclosed to the agency to notify it of the status of the case or matter or of any decision or determination that has been made or to make such other inquiries and reports as are necessary during the processing of the case or matter.

6. A record relating to a case or matter may be disclosed to a foreign country pursuant to an international treaty or convention entered into and ratified by the United States, or to an Executive agreement.

7. A record may be disclosed to a Federal, State, local, foreign, or international law enforcement agency to assist in crime prevention and detection or to provide leads for investigation.

8. A record may be disclosed to a Federal, State, local, foreign, tribal or other public authority in response to its request in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuing of a license, grant, or other benefit by the requesting agency, to the extent that the information relates to the requesting agency's decision on the matter.

9. A record may be disclosed to the public, news media, trade associations, or organized groups when the purpose is educational or informational, such as describing crime trends or distinctive or unique modus operandi, provided that the record does not identify a specific individual.

10. A record may be disclosed to an appeal or grievance examiner, formal complaints examiner, equal opportunity