

is a party before a court or administrative body.

j. To an appeal, grievance, hearing, or complaints examiner; an equal employment opportunity investigator, arbitrator, or mediator; and/or an exclusive representative or other person authorized to investigate or settle a grievance, complaint, or appeal filed by an individual who is the subject of the record.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Computer records are stored on a secure server and accessed over the Web via encryption software. Paper records, when created, are kept in file folders and cabinets in secure rooms. When individuals download information it is kept on encrypted computers that are accessed using PIV credentials. It is their responsibility to protect the data, including compliance with HCO 2180.1, GSA Rules of Behavior for Handling Personally Identifiable Information (PII).

RETRIEVABILITY:

Records are retrievable by a combination of first name and last name. Group records are retrieved by organizational code or other listed identifiers as configured in the application by the program office for their program requirements.

SAFEGUARDS:

Cloud systems are authorized to operate separately by the GSA CIO at the moderate level. All GSA Users utilize two-factor authentication to access Google Apps and Salesforce.com. Access is limited to authorized individuals with passwords or keys. Computer records are protected by a password system that is compliant with National Institute of Standards and Technology standards. Paper records are 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 retained and disposed of according to GSA records maintenance and disposition schedules, GSA Records Maintenance and Disposition System (CIO P 1820.1), GSA 1820.2A, and requirements of the National Archives and Records Administration.

SYSTEM MANAGER AND ADDRESS:

Director, Office of Enterprise Solutions, General Services Administration, 1800 F Street NW., Washington, DC 20405.

NOTIFICATION PROCEDURE:

An individual can determine if this system contains a record pertaining to him/her by sending a request in writing, signed, to the System Manager at the above address. When requesting notification of or access to records covered by this notice, an individual should provide his/her full name, date of birth, region/office, and work location. An individual requesting notification of records in person must provide identity documents sufficient to satisfy the custodian of the records that the requester is entitled to access.

RECORD ACCESS PROCEDURES:

Individuals wishing to access their own records should contact the system manager at the address above.

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 information in the system are the individuals about whom the records are maintained, the supervisors of those individuals, existing GSA systems, a sponsoring agency, a former sponsoring agency, other Federal agencies, contract employers, or former employers.

[FR Doc. 2014-19071 Filed 8-11-14; 8:45 am]

BILLING CODE 6820-14-P

GENERAL SERVICES ADMINISTRATION

[Notice-CIB-2014-02; Docket No. 2014-0002; Sequence No. 22]

Privacy Act of 1974; Notice of Updated Systems of Records

AGENCY: General Services Administration.

ACTION: Notice.

SUMMARY: GSA reviewed its Privacy Act systems to ensure that they are relevant, necessary, accurate, up-to-date and covered by the appropriate legal or regulatory authority. This notice is an updated Privacy Act system of records notice.

DATES: September 11, 2014.

ADDRESSES: GSA Privacy Act Officer (ISP), General Services Administration, 1800 F Street NW., Washington, DC 20405.

FOR FURTHER INFORMATION CONTACT: Call or email the GSA Privacy Act Officer telephone 202-208-1317; email gsa.privacyact@gsa.gov.

SUPPLEMENTARY INFORMATION: GSA undertook and completed an agency-

wide review of its Privacy Act systems of records. As a result of the review, GSA is publishing an updated Privacy Act system of records notice.

The revised system notice reflects additional data that is collected and stored within the system. This update does not change individuals' rights to access or amend their records in the system of records.

Dated: August 7, 2014.

James L. Atwater,

Director, Policy and Compliance Division, Office of the Chief Information Officer.

GSA/CIO-1

SYSTEM NAME:

GSA Credential and Identity Management System (GCIMS).

SYSTEM LOCATION:

GCIMS comprises a web-based application and data is maintained in a secure server facility in Fort Worth, TX and Kansas City, MO. Additionally, some fingerprint data may be stored in other GSA facilities to handle adjudications for employees and contractors located in GSA facilities where staffed fingerprint collection stations have been established to handle the contractor and employee Personal Identity Verification (PIV) process. Contact the System Manager for additional information.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals who require routine access to agency facilities and information technology systems, including:

- a. Federal employees.
- b. Contractors.
- c. Child care workers and other temporary workers with similar access requirements.

The system does not apply to occasional visitors or short-term guests, to whom GSA facilities may issue local Facility Access Cards (FAC).

CATEGORIES OF RECORDS IN THE SYSTEM:

The system contains information needed for issuing and maintaining HSPD-12 credentials and also access privilege information. Records may include:

- Employee/contractor/other worker full name
- Social Security Number (SSN)
- Date of birth
- Place of birth
- Height
- Weight
- Hair color
- Eye color
- Sex
- Citizenship

- Non-US citizens only:
 - Port of entry city and state
 - Date of entry
 - Less than 3-year US resident (yes or no)
- Occupation
- Summary report of investigation
- Investigation results and date
- File attachments containing PII
- Security Specialist Notes
- Investigation History Data
- Level of security clearance
- Date of issuance of security clearance
- Facial Image
- Fingerprints
- Organization/office of assignment
- Region
- Company name
- Telephone number
- ID card issuance and expiration dates
 - ID card number
 - Emergency responder designation
 - Home address and work location
 - Emergency contact information
 - Physical and logical access
 - Contractors only:
 - Contract company (also referred as vendor)
 - Vendor Point of Contact (POC)
 - Whether contract company is the prime or a subcontractor
 - Name of prime if company is subcontractor
 - Task order number, delivery order, or contract base number
 - Contract start and end date
 - Contract option years (yes or no)
 - Names of previous companies on GSA contracts

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301, 40 U.S.C. 121, 40 U.S.C. 582, 40 U.S.C. 3101, 40 U.S.C. 11315, 44 U.S.C. 3602, E.O. 9397, as amended, and Homeland Security Presidential Directive 12 (HSPD-12).

PURPOSE:

The primary purposes of the system are: To act as an authoritative source for GSA identities including employees and contractors to verify that all persons requiring routine access to GSA facilities or using GSA information resources have sufficient background investigations and are permitted access, to track and manage PIV smart cards issued to persons who have routine access to GSA facilities and information systems, to provide reports of identity data for administrative and staff offices to efficiently track and manage personnel, and to track and process background investigations for GSA personnel. (GSA branded the PIV card that it issues to its personnel as the GSA Access Card.)

ROUTINE USES OF THE SYSTEM RECORDS, INCLUDING CATEGORIES OF USERS AND THEIR PURPOSE FOR USING THE SYSTEM:

System information may be accessed and used by:

a. *GSA Personnel and GSA investigation service provider Department of Homeland Security, Federal Protective Service (DHS FPS) Personnel when needed for official use only, including, but not limited to: managing identity information of GSA personnel; managing the issuance and maintenance of Access Cards; managing the completion of background investigation requirements.*

Additional users who do not have access to privacy data are:

- *IT Helpdesk Personnel.*
- *Building Managers controlling physical access.*
- *System Administrators providing logical access.*
- *Record Holders updating their personal information (Employment Information, Emergency Contacts, Work and Home Address) in the self-service module.*
- *Google Mail Team.*

b. To verify suitability of an employee or contractor before granting access to specific resources;

c. To disclose information to agency staff and administrative offices who may restructure the data for management purposes;

d. An authoritative source of identities for Active Directory, Google mail, and other GSA systems;

e. In any legal proceeding, where pertinent, to which GSA is a party before a court or administrative body;

f. To authorized officials engaged in investigating or settling a grievance, complaint, or appeal filed by an individual who is the subject of the record.

g. To a Federal, state, local, foreign, or tribal agency in connection with the hiring or retention of an employee; the issuance of a security clearance; the reporting of an investigation; the letting of a contract; or the issuance of a grant, license, or other benefit to the extent that the information is relevant and necessary to a decision;

h. To the Office of Personnel Management (OPM), the Office of Management and Budget (OMB), or the Government Accountability Office (GAO) when the information is required for program evaluation purposes;

i. To a Member of Congress or staff on behalf of and at the request of the individual who is the subject of the record;

j. To an expert, consultant, or contractor of GSA in the performance of a Federal duty to which the information is relevant;

k. To the National Archives and Records Administration (NARA) for records management purposes;

l. To appropriate agencies, entities, and persons when (1) the Agency suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Agency has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by GSA or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with GSA's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING RECORDS IN THE SYSTEM:**STORAGE:**

Computer records are stored on a secure server and accessed over the web using encryption software. Paper records, when created, are kept in file folders and cabinets in secure locked rooms where only authorized personnel have access. The enrollment workstations are kept in secure locations with limited access to authorized personnel only.

RETRIEVABILITY:

Records are retrievable by a combination of first name, last name, and/or Social Security Number. Group records are retrieved by organizational code.

SAFEGUARDS:

Computer records within GCIMS are protected utilizing certificate based smart card login. Paper records are 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 as specified in the handbook, GSA Records Maintenance and Disposition System (CIO P 1820.1).

SYSTEM MANAGER AND ADDRESS:

Program Manager, Identity, Credential and Access Management Division, General Services Administration, 1800 F St. NW., Room 2340, Washington, DC 20405.

NOTIFICATION PROCEDURE:

Individuals wishing to inquire if the system contains information about them should contact the system manager at the above address.

CONTESTING RECORD PROCEDURES:

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

RECORD SOURCES CATEGORIES:

The sources for information in the system are the individuals about whom the records are maintained, the supervisors of those individuals, existing GSA systems, sponsoring agency, former sponsoring agency, other Federal agencies, contract employer, former employer, and the U.S. Office of Personnel Management (OPM).

[FR Doc. 2014–19079 Filed 8–11–14; 8:45 am]

BILLING CODE 6820–20–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Declaration Regarding Emergency Use of In Vitro Diagnostics for Detection of Ebola Virus

AGENCY: Office of the Secretary, Department of Health and Human Services.

ACTION: Notice.

SUMMARY: The Secretary of Health and Human Services (HHS) is issuing this notice pursuant to section 564 of the Federal Food, Drug, and Cosmetic (FD&C) Act, 21 U.S.C. 360bbb–3. On September 22, 2006, then Secretary of Homeland Security, Michael Chertoff, determined pursuant to section 319F–2 of the Public Health Service Act, 42 U.S.C. 247d–6b, that the Ebola virus presents a material threat against the United States population sufficient to affect national security.

On the basis of this determination, on August 4, 2014 the Secretary declared that circumstances exist justifying the authorization of emergency use of *in vitro* diagnostics for detection of Ebola virus pursuant to section 564 of the FD&C Act, subject to the terms of any authorization issued under that section.

DATES: The determination and declaration are effective August 4, 2014.

FOR FURTHER INFORMATION CONTACT: Nicole Lurie, M.D., MSPH, Assistant Secretary for Preparedness and Response, Office of the Secretary, Department of Health and Human Services, 200 Independence Avenue SW., Washington, DC 20201, Telephone (202) 205–2882 (this is not a toll-free number).

SUPPLEMENTARY INFORMATION:**I. Background**

Under Section 564 of the FD&C Act, the Commissioner of the Food and Drug Administration (FDA), acting under delegated authority from the Secretary of HHS, may issue an Emergency Use Authorization (EUA) authorizing (1) the emergency use of an unapproved drug, an unapproved or uncleared device, or an unlicensed biological product; or (2) an unapproved use of an approved drug, approved or cleared device, or licensed biological product. Before an EUA may be issued, the Secretary of HHS must declare that circumstances exist justifying the authorization based on one of four determinations: (1) A determination by the Secretary of Homeland Security that there is a domestic emergency, or a significant potential for a domestic emergency, involving a heightened risk of attack with a biological, chemical, radiological, or nuclear (“CBRN”) agent or agents; (2) the identification of a material threat by the Secretary of Homeland Security pursuant to section 319F–2 of the Public Health Service (PHS) Act¹ sufficient to affect national security or the health and security of United States citizens living abroad; (3) a determination by the Secretary of Defense that there is a military emergency, or a significant potential for a military emergency, involving a heightened risk to United States military forces of attack with a CBRN agent or agents; or (4) a determination by the Secretary that there is a public health emergency, or a significant potential for a public health emergency, that affects, or has a significant potential to affect, national security or the health and security of United States citizens living abroad, and that involves a CBRN agent or agents, or a disease or condition that may be attributable to such agent or agents.

Based on any of these four determinations, the Secretary of HHS may then declare that circumstances exist that justify the EUA, at which point the FDA Commissioner may issue an EUA if the criteria for issuance of an authorization under section 564 of the FD&C Act are met.

The Department of Defense requested that the FDA issue an EUA for *in vitro* diagnostics for detection of Ebola virus

¹ 42 U.S.C. 247d–6b, which states: “[t]he Homeland Security Secretary, in consultation with the Secretary and the heads of other agencies as appropriate, shall on an ongoing basis—(i) assess current and emerging threats of chemical, biological, radiological, and nuclear agents; and (ii) determine which of such agents present a material threat against the United States population sufficient to affect national security.”

to allow the Defense Department to take preparedness and response measures based on information currently available about the Ebola virus in Western Africa. The material threat determination by the Secretary of Homeland Security, and the declaration that circumstances exist justifying emergency use of *in vitro* diagnostics for detection of Ebola virus by the Secretary of HHS, as described below, enable the FDA Commissioner to issue an EUA for certain *in vitro* diagnostics for emergency use under section 564 of the FD&C Act.

II. Material Threat Determination by the Secretary of Homeland Security

On September 22, 2006, then Secretary of Homeland Security, Michael Chertoff, determined pursuant to section 319F–2 of the Public Health Service Act, 42 U.S.C. 247d–6b, that the Ebola virus presents a material threat against the United States population sufficient to affect national security.

III. Declaration of the Secretary of Health and Human Services

On August 4, 2014, on the basis of the Secretary of Homeland Security’s determination that the Ebola virus presents a material threat against the United States population sufficient to affect national security, I declared that circumstances exist justifying the authorization of emergency use of *in vitro* diagnostics for detection of Ebola virus pursuant to section 564 of the FD&C Act, subject to the terms of any authorization issued under that section.

Notice of the EUAs issued by the FDA Commissioner pursuant to this determination and declaration will be provided promptly in the **Federal Register** as required under section 564 of the FD&C Act.

Dated: August 5, 2014.

Sylvia M. Burwell,
Secretary.

[FR Doc. 2014–19026 Filed 8–11–14; 8:45 am]

BILLING CODE 4150–37–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Meeting of the National Vaccine Advisory Committee

AGENCY: National Vaccine Program Office, Office of the Assistant Secretary for Health, Office of the Secretary, Department of Health and Human Services.

ACTION: Notice.

SUMMARY: As stipulated by the Federal Advisory Committee Act, the Department of Health and Human