TRANSACTION GRANTED EARLY TERMINATION—Continued

ET date	Trans No.	ET req status	Party name
		G	Greenpium, Inc.
	20100881	G	POSCO.
		G	Daewoo International Corporation.
		G	Daewoo International Corporation.
	20100882	G	Sanofi-Aventis.
		G	Metabolex, Inc.
		G	Metabolex, Inc.
21–JUL–10	20100886	G	Wayzata Opportunities Fund, LLC.
		G	Entegra Power Group LLC.
		G	Gila River Power, L.P.
	20100892	G	Avon Products, Inc.
		G	Gerald A. Kelly, Jr. and Bonnie C. Kelly.
		G	Silpada Designs, Inc.
22–JUL–10	20100856	G	Marfrig Alimentos S.A.
		G	LGB Keystone LLC.
		G	Keystone Foods Intermediate LLC.
	20100863	Y	Ocwen Financial Corporation.
		Y	Barclays PLC.
		Y	BCRE.
	20100878	G	Biovail Corporation.
		G	Valeant Pharmaceuticals International.
		G	Valeant Pharmaceuticals International.
	20100880	G	GTCR Fund IX/A, L.P.
		G	UCB S.A.
		G	UCB, Inc.
	20100891	G	Communications Infrastructure Investments, LLC.
		G	American Fiber Systems Holding Corp.
		G	American Fiber Systems Holding Corp.
	20100896	G	Roper Industries, Inc.
		G	ITN Holdings, LLC.
		G	iTradeNetwork, Inc.
23–JUL–10	20100868	G	Anchorage Capital Partners Offshore, Limited.
		G	Hampton Roads Bankshares, Inc.
		G	Hampton Roads Bankshares, Inc.
	20100895	G	AIF VII Euro Holdings, L.P.
		G	Carib Holdings, Inc.
		G	Carib Holdings, Inc.
	20100899	G	Crown Castle International Corp.
		G	NewPath Networks, Inc.
		G	NewPath Networks, Inc.
	20100903	G	PPL Corporation.
		G	E. ON AG.
		G	E. ON U.S. LLC.
	20100906	G	JSC Atomredmetzoloto.
		G	Uranium One, Inc.
		G	Uranium One, Inc.
	20100908	G	ZM Capital, L.P.
		G	Alloy, Inc.
		G	Alloy, Inc.
	20100916	G	DCP Midstream Partners, L.P.
		G	UGI Corporation.
		G	Atlantic Energy, Inc.
	20100918	G	Bank of America Corporation.
		G	Sentinel Capital Partners III, L.P.
		G	Strategic Partners Holdings, Inc.

FOR FURTHER INFORMATION CONTACT:

Sandra M. Peay, Contact Representative,

Or

Renee Chapman, Contact Representative.

Federal Trade Commission, Premerger Notification Office, Bureau of Competition, Room H–303, Washington, DC 20580, (202) 326–3100.

By Direction of the Commission.

Donald S. Clark,

Secretary.

[FR Doc. 2010–19361 Filed 8–6–10; 8:45 am]

BILLING CODE 6750–01–M

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of Security and Strategic Information

Privacy Act of 1974; Report of a New System of Records

AGENCY: Office of the Assistant Secretary for Administration and Management.

ACTION: Notice of a New Privacy Act System of Records.

SUMMARY: In accordance with the requirements of the Privacy Act of 1974, the Department of Health and Human Services is establishing a new system of records entitled, "Facility and Resource Access Control Records," System No. 09–90–0777. This notice implements in part Homeland Security Presidential Directive 12 (HSPD–12), "Policy for a Common Identification Standard for Federal Employees and Contractors" of August 27, 2004. HSPD–12 requires all employees, contractors, and others who will be granted regular access to federal facilities for more than six months to undergo a background investigation to determine suitability and to be issued a Personal Identity Verification (PIV) Card (*i.e.* an identification badge). The purpose of the program is to enhance access controls to federal facilities to improve security. The badge stores the individual's name, employing organization, the badge issuer, the badge serial number, the expiration date, a picture of the badge holder, two fingerprints, and four encryption keys that may be used by the PIV card holder, when properly activated, in association with federal information technology resources. The Facility and Resource Access Control Records comprise information about the issuance of Personal Identity Verification (PIV) cards, PIV card holders (*e.g.* employees, contractors), other individuals who require regular access to HHS facilities or resources, and the use of PIV cards to access facilities or resources. The Facility and Resource Access Control Records also include information about occasional visitors and short-term guests who do not carry PIV cards but to whom HHS will issue temporary credentials.

DATES: *Effective Date:* The new system of records will be effective on the date of publication of this notice, with the exception of the routine uses, which will become effective on September 8, 2010. We may defer implementation of this system or one or more of the routine use statements listed below if we receive comments that persuade us to do so.

DATES: Comments are due by September 8, 2010.

ADDRESSES: Address comments to HHS Privacy Act Officer, Mary E. Switzer Building, Department of Health and Human Services, 330 "C" Street, SW., Washington, DC 20201, or via electronic mail to HSPD12-privacy at hhs.gov. Comments will be available for public viewing in the public reading room located at the same address, or on our Web site at *http://www.hhs.gov.* To review comments in person, please call the Division of Freedom of Information and Privacy at 202–690–7453 for an appointment.

FOR FURTHER INFORMATION CONTACT: Ms. Maya A. Bernstein, Office of the Assistant Secretary for Planning and Evaluation, 200 Independence Avenue, SW., Room 434E, Washington, DC 20201, via e-mail at *maya.bernstein@hhs.gov,* or via telephone at 202/690–7100.

SUPPLEMENTARY INFORMATION: The Facility and Resource Access Control Records enhance HHS' security and permit the Department to comply with Homeland Security Presidential Directive 12 (HSPD–12), "Policy for a Common Identification Standard for Federal Employees and Contractors." This Presidential mandate requires all government employees, contractors, and certain other individuals to use new identification badges, known as Personal Identity Verification (PIV) cards, as their singular form of identification when accessing government buildings, facilities, or information technology systems. The PIV card will enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy.

Before obtaining a PIV card, each employee or contractor must undergo a standardized security credentialing process, including background investigations, to ensure safety of HHS facilities and the people who work in them. The PIV card system places modern card readers at the entrances of HHS facilities that allow interoperability with all federal agencies and ensure that entry of employees, contractors, and other regular visitors is strictly authorized. Leveraging cutting-edge technologies such as fingerprint recognition and single sign-on capabilities, this technology will reduce identity fraud and ensure only authorized users can access essential information. Finally, by protecting employees, facilities, and information, the PIV card guards the government resources that provide critical services to the American people.

The PIV card will store the holder's name, employing organization, the badge issuer, the badge serial number, the expiration date, a picture of the badge holder, two fingerprints, and encryption keys that may be activated for access to information technology resources, if needed. It will not store other identifying information such as social security number or birth date. An associated database will store similar information in order to verify that individuals entering federal buildings or using other federal resources, such as information technology (IT) systems, are properly authorized for that access. In addition, the database will be used to verify the ability of other agencies' PIV card holders to enter HHS facilities or use HHS resources.

Although HHS will not issue PIV cards to occasional visitors, information about occasional visitors will be maintained as part of the Facility and Resource Access Control Records. Some of these visitors may be required to undergo brief criminal history checks, depending on the reason for their visit and how often they enter our facilities or use our (IT) systems. The Facility and Resource Access Control Records includes that information.

Routine Uses

In addition to the collection, use, and disclosure of information described in the statute itself, the Privacy Act permits HHS to establish disclosures to non-HHS entities that are not already identified by statute, and do not require the individual record subject's consent, by using an administrative process. These disclosures are known as "routine uses," and are permitted to be established if they are "compatible with the purpose" for which the information was collected, and if the agency publishes them in the **Federal Register** for 30 days in advance. Both identifiable and non-identifiable data may be disclosed under a routine use. This notice includes routine uses for the new system, and they are described below.

Most of the routine uses fall into standard categories that are common to most systems of records across the government. These include (1) disclosure to the Department of Justice (DOJ) when DOJ represents HHS, our employees, or the government in litigation, and they need to have access to the records to perform that function. If such a case goes to court, another routine use (2) permits the records to be disclosed in evidence before a federal court or appropriate adjudicative body. There is a disclosure (3) permitted when a record in this system of records or in combination with other records indicates a violation of law — we turn them over to the appropriate law enforcement entity in order to maintain the integrity of the program and ensure trust in the system. Another routine use (4) permits disclosure for intelligence and national security purposes, especially since the system manages information about persons that have access to federal facilities and federal information technology systems that has

been recognized by the President as a homeland security issue.

The routine use disclosure to an individual Member of Congress (5) permits the Department to cooperate with a Member of Congress seeking information on behalf of a constituent (as opposed to the Committees of jurisdiction performing oversight) with a matter that involves these records. If the request is in writing, and we obtain a copy of the request, we will assume the constituent's consent for the Member to obtain records on a constituent's behalf even if a formal authorization is not included, so that the Department and the Member can better serve our citizens. However, the Member would get no more access to the record than that to which the constituent is entitled.

The sixth routine use (6) permits the National Archives and Records Administration to carry out records management functions.

Where HHS engages a contractor to carry out a function related to this system of records, routine use (7) permits disclosure to those individuals who require access to the records in order to perform the contracted work, and we will require the contractor to comply with the Privacy Act. Another routine use (8) permits disclosure to contractors or other agencies for the purpose of assisting the Department in responding to a suspected or confirmed data breach.

When an individual submits an application for a background investigation, the individual normally signs an authorization permitting records to be obtained by the investigator from almost any source. Occasionally, after an individual has moved to another job or contract, if negative information should come to light relevant to another entity's decision about the suitability of the individual, a routine use (9) allows HHS to notify the other entity merely that we have relevant information. It is expected that the other entity, if interested in pursuing the matter, would present a written authorization on which HHS could rely to disclose more detailed records. However, the disclosed information will be limited to that which is reliable enough for such a referral.

Finally, one routine use is particular to the PIV card system and allows the program to function as it is intended. HSPD–12 directs that, eventually, all PIV card holders should, in most cases, be able to visit other federal facilities and, if appropriate, use other agencies' computer resources, by presenting the PIV card. This system of records also describes information about visitors to HHS who have a PIV card from another agency. Therefore, this system of records also comprises information about those visitors, their entry and exit times, and summary information about them. A routine use (10) permits HHS to notify another federal agency if a PIV card is expired or no longer valid.

Safeguards

HHS has safeguards in place for authorized users and monitors such users to ensure against excessive or unauthorized use. Personnel having access to the system have been trained in the Privacy Act and information security requirements. Employees who maintain records in this system are instructed not to release data until the intended recipient agrees to implement appropriate management, operational and technical safeguards sufficient to protect the confidentiality, integrity and availability of the information and information systems and to prevent unauthorized access.

This system will conform to all applicable federal laws and regulations and federal and HHS policies and standards as they relate to information security and data privacy. These laws and regulations may apply but are not limited to: the Privacy Act of 1974; the Federal Information Security Management Act of 2002; the Computer Fraud and Abuse Act of 1986; the Health Insurance Portability and Accountability Act of 1996; the E–Government Act of 2002, and the Clinger-Cohen Act of 1996 Circular A–130, Management of Federal Resources, Appendix III, Security of Federal Automated Information Resources also applies. Federal, and HHS policies and standards include but are not limited to: all pertinent National Institute of Standards and Technology publications and the HHS Information Systems Program Handbook.

Dated: July 26, 2010.

RADM Arthur J. Lawrence,

Director, Office of Security and Strategic Information.

SYSTEM NO. 09–90–0777

SYSTEM NAME:

"Facility and Resource Access Control Records".

SECURITY CLASSIFICATION:

Most identity records are not classified. However, in some cases, records of certain individuals, or portions of some records, may be classified in the interest of national security.

SYSTEM LOCATION:

Data covered by this system are maintained at the following locations: Department of Health and Human Services (HHS), Office of the Secretary, 200 Independence Avenue, SW., Washington, DC 20201; HHS Operating Divisions and regional offices around the country; Qwest Datacenter in Sterling, Virginia; and the Qwest CyberCenter in Highlands Ranch, Colorado. Some data covered by this system will be accessed at HHS locations, both federal buildings and federally-leased space, and at the physical security office(s) or computer security offices of those locations.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

(1) Individuals who require or are under consideration to obtain regular, ongoing access to HHS facilities, information technology systems, or information classified in the interest of national security, such as applicants for employment or contracts with HHS, federal employees, tribal members, contractors, students, interns, volunteers, affiliates such as individuals authorized to perform or use services provided in HHS facilities (*e.g.,* HEW Credit Union, fitness center, etc.) and individuals formerly in any of these positions. (2) PIV card holders from other agencies who visit HHS facilities or use HHS computer systems. (3) Occasional visitors or short-term employees or guests who do not carry PIV cards and do not require certificates for using encryption with a Public Key Infrastructure (PKI), to whom HHS will issue temporary identification and low assurance credentials.

CATEGORIES OF RECORDS IN THE SYSTEM:

(1) Records maintained on individuals issued credentials by HHS include the following: Full name, Social Security number; date and place of birth; citizenship; signature; image (photograph); fingerprints; hair color; eye color; height; weight; sex; race; scars, marks, or tattoos; organization/office of assignment, location and contact information; PIV card issue and expiration dates; personal identification number (PIN); PIV request form; PIV sponsor, enrollment, registrar and issuance information; PIV card serial number; emergency responder designation; foreign national designator; contractor designator; information derived from documents used to verify identity such as document title, issuing authority, or expiration date; position sensitivity; level of national security clearance and expiration date; computer system user name; user access and

permission rights; authentication certificates; digital signature information; employment category; position title; dates, times, and locations of entries and exits.

(2) HHS maintains the following categories of records about PIV card holders from other agencies entering HHS facilities or using HHS systems: Name, PIV card serial number; dates, times, and locations of entries and exits; organization name; level of national security clearance and expiration date; digital signature information; computer networks, applications, and data accessed.

(3) HHS maintains the following categories of records about occasional visitors and short term guests: name, photograph, date and time of entry and exit, facility to which admitted, and name of person visiting.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301; Information Technology Management Reform Act of 1996 (Pub. L. 104–106, sec. 5113); Electronic Government Act (Pub. L. 104–347, sec. 203); Paperwork Reduction Act of 1995 (44 U.S.C. ch. 35); Government Paperwork Elimination Act (Pub. L. 105–277, sec. 1701, 44 U.S.C. 3504); Homeland Security Presidential Directive (HSPD) 12, Policy for a Common Identification Standard for Federal Employees and Contractors, Aug. 27, 2004; Federal Property and Administrative Act of 1949, as amended.

PURPOSE(S) OF THE SYSTEM:

The primary purposes of the system of records are to (1) Ensure the safety and security of HHS facilities, systems, or information, and our occupants and users; (2) to verify that all persons entering federal facilities, using federal information resources, or accessing classified information are authorized to do so; and (3) to track and control PIV cards and other identity credentials issued to persons entering and exiting the facilities, using systems, or accessing classified information.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OR USERS AND THE PURPOSES OF SUCH USES:

Information about covered individuals may be disclosed without consent as permitted by the Privacy Act of 1974, 5 U.S.C. 552a(b), and:

(1) To the Department of Justice when: (a) The agency or any component thereof; or (b) any employee of the agency in his or her official capacity; (c) any employee of the agency in his or her individual capacity where agency or the Department of Justice has agreed to represent the employee; or (d) the United States government, is a party to litigation or has an interest in such litigation, and by careful review, the agency determines that the records are both relevant and necessary to the litigation and the use of such records by DOJ is therefore deemed by the agency to be for a purpose compatible with the purpose for which the agency collected the records.

(2) To a court or adjudicative body in a proceeding when: (a) The agency or any component thereof; (b) any employee of the agency in his or her official capacity; (c) any employee of the agency in his or her individual capacity where agency or the Department of Justice has agreed to represent the employee; or (d) the United States government, is a party to litigation or has an interest in such litigation, and by careful review, the agency determines that the records are both relevant and necessary to the litigation and the use of such records is therefore deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records.

(3) Except as noted on Forms SF 85, 85–P, and 86, when a record on its face, or in conjunction with other records, indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule, or order issued pursuant thereto, disclosure may be made to the appropriate public authority, whether federal, foreign, state, local, or tribal, or otherwise, responsible for enforcing, investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation, or order issued pursuant thereto, if the information disclosed is relevant to any enforcement, regulatory, investigative or prosecutorial responsibility of the receiving entity.

(4) To a federal, state, or local agency, or other appropriate entities or individuals, or through established liaison channels to selected foreign governments, in order to enable an intelligence agency to carry out its responsibilities under the National Security Act of 1947 as amended, the CIA Act of 1949 as amended, Executive Order 12333 or any successor order, applicable national security directives, or classified implementing procedures approved by the Attorney General and promulgated pursuant to such statutes, orders or directives.

(5) To a Member of Congress or to a Congressional staff member in response to an inquiry of the Congressional office made at the written request of the constituent about whom the record is maintained.

(6) To the National Archives and Records Administration or to the General Services Administration for records management inspections conducted under 44 U.S.C. 2904 and 2906.

(7) To agency contractors who have been engaged to assist the agency in the performance of a contract service, grant, cooperative agreement, or other activity related to this system of records and who need to have access to the records in order to perform the activity. Recipients shall be required to comply with the requirements of the Privacy Act of 1974, as amended, 5 U.S.C. 552a.

(8) To appropriate federal agencies and Department contractors that have a need to know the information for the purpose of assisting the Department's efforts to respond to a suspected or confirmed breach of the security or confidentiality of information maintained in this system of records, and the information disclosed is relevant and necessary for that assistance.

(9) To a federal, state, local, foreign, or tribal or other public authority the fact that this system of records contains information relevant to the retention of an employee, the retention of a security clearance, the letting of a contract, or the issuance or retention of a license, grant, or other benefit. The other agency or licensing organization may then make a request supported by the written consent of the individual for the entire record if it so chooses. No disclosure will be made unless the information has been determined to be sufficiently reliable to support a referral to another office within the agency or to another federal agency for criminal, civil, administrative personnel or regulatory action.

(10) To another federal agency to notify that agency when, or verify whether, a PIV card is no longer valid.

Note: Disclosures of data pertaining to date and time of entry and exit of an agency employee working in the District of Columbia may not be made to supervisors, managers or any other persons (other than the individual to whom the information applies) to verify employee time and attendance record for personnel actions because 5 U.S.C. 6106 prohibits federal Executive agencies (other than the Bureau of Engraving and Printing) from using a recording clock within the District of Columbia, unless used as a part of a flexible schedule program under 5 U.S.C. 6120 *et seq.*

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

STORAGE:

Records are stored in electronic media and in paper files.

RETRIEVABILITY:

Records are retrievable by name, date of birth, Social Security number, photographic identifiers, biometric identifiers, HHS Identification Number, and PIV card serial numbers.

SAFEGUARDS:

HHS has safeguards in place for authorized users and monitors such users to ensure against excessive or unauthorized use. Personnel having access to the system have been trained in the Privacy Act and information security requirements. Employees who maintain records in this system are instructed not to release data until the intended recipient agrees to implement appropriate management, operational and technical safeguards sufficient to protect the confidentiality, integrity and availability of the information and information systems and to prevent unauthorized access.

This system will conform to all applicable federal laws and regulations and federal and HHS policies and standards as they relate to information security and data privacy. These laws and regulations may apply but are not limited to: the Privacy Act of 1974; the Federal Information Security Management Act of 2002; the Computer Fraud and Abuse Act of 1986; the Health Insurance Portability and Accountability Act of 1996; the E-Government Act of 2002, the Clinger-Cohen Act of 1996; the Medicare Modernization Act of 2003, and the corresponding implementing regulations. OMB Circular A–130, Management of Federal Resources, Appendix III, Security of Federal Automated Information Resources also applies. Federal, and HHS policies and standards include but are not limited to: All pertinent National Institute of Standards and Technology publications and the HHS Information Systems Program Handbook.

Paper records are kept in locked cabinets in secure facilities and access to them is restricted to individuals whose role requires use of the records. The computer servers in which records are stored are located in facilities that are secured by alarm systems and off-master key access. The computer servers themselves are two-factor protected with Public Key Infrastructure (PKI) credentials, Personal Identification Numbers (PINs) and passwords. Access to individuals working at guard stations, operating enrollment stations, issuance stations, or the portal for sponsorship and adjudication will be two-factor protected using PKI and PIN; each person granted access to the system at guard stations, enrollment stations, issuance stations or through the portal must be individually authorized to use the system. A notice warning users that they are responsible for protecting the information in accordance with the Privacy Act, the Computer Security Act, and the Federal Information Security Management Act appears on the monitor screen when records containing information on individuals are first displayed. Data exchanged between the servers and the personal computers at the guard stations and badging office are encrypted. Backup tapes are stored in a locked and controlled room in a secure, off-site location.

An audit trail is maintained and reviewed periodically to identify unauthorized access. Persons given roles in the PIV process must complete training specific to their roles to ensure they are knowledgeable about how to protect individually identifiable information.

RETENTION AND DISPOSAL:

Records relating to persons' access covered by this system are retained in accordance with General Records Schedule 18, Item 17 approved by the National Archives and Records Administration (NARA). Unless retained for specific, ongoing security investigations, for maximum security facilities, records of access are maintained for five years and then destroyed. For other facilities, records are maintained for two years and then destroyed.

All other records relating to individuals are retained and disposed of in accordance with General Records Schedule 18, item 22, approved by NARA. In accordance with HSPD–12, PIV cards are deactivated within 18 hours of cardholder separation, loss of card, or expiration. PIV cards are destroyed by cross-cut shredding no later than 90 days after deactivation.

SYSTEM MANAGER AND ADDRESS:

Ken Calabrese, HHS Chief Technology Officer, Office of the HHS Chief Information Officer, Department of Health and Human Services, 200 Independence Avenue, SW., Washington, DC 20201.

NOTIFICATION PROCEDURE:

An individual can determine if this system contains a record pertaining to himself or herself by sending a request in writing, signed, to HHS Privacy Act Officer, Room 2221, Mary E. Switzer Building, Department of Health and Human Services, 330 "C" Street, SW., Washington, DC 20201. When requesting notification of or access to records covered by this Notice, an individual should provide his/her full name, date of birth, agency name, 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, such as a government-issued photo ID. Individuals requesting notification via telephone must furnish, at a minimum, name, date of birth, social security number, and home address in order to establish identity. Individuals requesting notification via mail shall submit a notarized request to the responsible Department official to verify his or her identity or shall certify in his or her request that he or she is the individual who he or she claims to be and that he or she understands that the knowing and willful request for or acquisition of a record pertaining to an individual under false pretenses is a criminal offense under the Act subject to a $5,000 fine.

RECORD ACCESS PROCEDURE:

In addition to the procedures above, requesters should reasonably specify the record contents being sought. If additional information or assistance is required, contact the HHS Privacy Act Officer, Room 2221, Mary E. Switzer Building, Department of Health and Human Services, 330 "C" Street, SW., Washington, DC 20201. Write the words "Privacy Act Request" on the envelope and on the letter. For purpose of access, use the same procedures outlined in the Notification Procedures above. (These procedures are in accordance with Department regulation 45 CFR 5b.5 (a)(2).)

CONTESTING RECORDS PROCEDURES:

In addition to the procedures above, requesters should also reasonably

identify the record, specify the information they are contesting, state the corrective action sought and the reasons for the correction along with supporting justification showing why the record is not accurate, timely, relevant, or complete. Rules regarding amendment of Privacy Act records appear in 45 CFR part 5a. If additional information or assistance is required, contact the HHS Privacy Act Officer, Room 2221, Mary E. Switzer Building, Department of Health and Human Services, 330 "C" Street, SW., Washington, DC 20201. Write the words "Privacy Act Request" on the envelope and on the letter.

RECORDS SOURCE CATEGORIES:

Employee, contractor, or applicant; sponsoring agency; former sponsoring agency; other federal agencies; contract employer; former employer.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

None.

[FR Doc. 2010–19536 Filed 8–6–10; 8:45 am]

BILLING CODE 4150–03–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Notice of Availability: Test Tools and Test Procedures Approved for the Office of the National Coordinator for Health Information Technology (ONC) Temporary Certification Program

AGENCY: Office of the National Coordinator for Health Information Technology, Office of the Secretary, Department of Health and Human Services.

ACTION: Notice.

Authority: 42 U.S.C. 300jj–11.

SUMMARY: This notice announces the availability of test tools and test procedures approved by the National Coordinator for Health Information Technology (the National Coordinator) for the testing of Complete EHRs and/or EHR Modules by ONC-Authorized Testing and Certification Bodies (ONC–ATCBs) under the ONC temporary certification program. The approved test tools and test procedures are identified on the ONC Web site at: *http://healthit.hhs.gov/certification*.

FOR FURTHER INFORMATION CONTACT: Carol Bean, Director, Certification Division, Office of the National Coordinator for Health Information Technology, 202–690–7151.

SUPPLEMENTARY INFORMATION:

On June 24, 2010, the Department of Health and Human Services issued a final rule establishing a temporary certification program for the purposes of testing and certifying health information technology ("Establishment of the Temporary Certification Program for Health Information Technology," 75 FR 36158) (Temporary Certification Program final rule).[1] The Temporary Certification Program final rule added a new "Subpart D—Temporary Certification Program for HIT" to part 170 of title 45 of the Code of Federal Regulations (CFR). Section 170.423(e) of Subpart D requires ONC–ATCBs to "[u]se test tools and test procedures approved by the National Coordinator for the purposes of assessing Complete EHRs and/or EHR Modules compliance with the certification criteria adopted by the Secretary." The preamble of the Temporary Certification Program final rule stated that when the National Coordinator had approved test tools and/or test procedures ONC would publish a notice of availability in the **Federal Register** and identify the approved test tools and test procedures on the ONC Web site. As discussed in the Temporary Certification Program final rule, we anticipated that test tools and test procedures would not be finalized by the National Institute of Standards and Technology (NIST), and therefore unable to be considered for approval by the National Coordinator, until after the Secretary made publicly available a final rule for the initial set of standards, implementation specifications, and certification criteria for electronic health record technology.[2] This final rule, "Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology" (HIT Standards and Certification Criteria final rule) was made available for public inspection on July 13, 2010, and was published in the **Federal Register** on July 28, 2010.

The National Coordinator has approved, for use by ONC–ATCBs in accordance with 45 CFR 170.423(e), test tools and test procedures developed by NIST for testing Complete EHRs and/or EHR Modules to the applicable certification criterion or criteria adopted by the Secretary in the HIT Standards and Certification Criteria final rule. These approved test tools and test procedures are identified on the ONC Web site at: *http://healthit.hhs.gov/certification*.

Dated: August 2, 2010.

David Blumenthal,

National Coordinator for Health Information Technology.

[FR Doc. 2010–19533 Filed 8–6–10; 8:45 am]

BILLING CODE 4150–45–P

[1] The Department issued a proposed rule entitled "Proposed Establishment of Certification Programs for Health Information Technology" (75 FR 11328, March 10, 2010) that proposed the establishment of a temporary certification program and a permanent certification program and stated the Department's intentions to issue separate final rules for each program.

[2] The "Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology" interim final rule was made available for public inspection on December 30, 2009, and published in the **Federal Register** on January 13, 2010 (75 FR 2014).

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Health Resources and Services Administration

Agency Information Collection Activities: Submission for OMB Review; Comment Request

Periodically, the Health Resources and Services Administration (HRSA) publishes abstracts of information collection requests under review by the Office of Management and Budget (OMB), in compliance with the Paperwork Reduction Act of 1995 (44 U.S.C. Chapter 35). To request a copy of the clearance requests submitted to OMB for review, e-mail *paperwork@hrsa.gov* or call the HRSA Reports Clearance Office on (301) 443–1129.

The following request has been submitted to the Office of Management and Budget for review under the Paperwork Reduction Act of 1995:

Proposed Project: Title: "Health Care and Other Facilities" Project Status Update Form (OMB No. 0915–0309)—[Extension] .

The Health Resources and Services Administration's Health Care and Other Facilities (HCOF) program provides congressionally-directed funds to health-related facilities for construction-related activities and/or capital equipment purchases. Awarded facilities are required to provide a periodic (quarterly for construction-related projects, annually for equipment only projects) update of the status of the funded project until it is completed. The monitoring period averages about 3 years, although some projects take up to 5 years to complete. The information collected from these updates is vital to program management staff to determine whether projects are progressing according to the established timeframes, meeting deadlines established in the Notice of Grant Award (NGA), and drawing down funds appropriately. The