System of Records Notices

Effective Date: September 19, 2016

COMMERCE/DEPT-25

SYSTEM NAME:

Access Control and Identity Management System.

SECURITY CLASSIFICATION:

Unclassified, sensitive, for official use only, and classified.

SYSTEM LOCATIONS:

a. For Office of Security, Office of the Secretary, U.S. Department of Commerce, Room 1033, 1401 Constitution Avenue NW., Washington, DC 20230.

b. For Office of Security, U.S. Census Bureau, Room 2J438, 4600 Silver Hill Road, Washington, DC 20233-3700.

c. For Office of Security, U.S. Census Bureau Indiana, Room 104, Building 66, 1201 E. 10th Street, Jeffersonville, IN 47132.

d. For Office of Security, National Institute of Standards and Technology, Room A-105, Building 318, 100 Bureau Drive, Gaithersburg, MD 20899.

e. For Office of Security, National Oceanic and Atmospheric Administration, Room G-101, SSMC-OFA543, 1335 East-West Highway, Silver Spring, MD 20910.

f. For Office of Security, National Oceanic and Atmospheric Administration, Western Region, Building 1, 7600 Sand Point Way NE., Seattle, WA 38115.

g. For Office of Security, FirstNet, John W. Powell Federal Building, 12201 Sunrise Valley, Drive, Reston, VA 22091.

h. For Office of Security, U.S. Patent and Trademark Office, 600 Dulany Street, Madison Building, West, Alexandria, Virginia 22313.

i. For Office of the Secretary, Minority Business Development Agency, Economic and Statistics Administration, and Economic Development Administration: Office of the Secretary, Chief Information Officer, 1401 Constitution Avenue NW., Washington, DC 20230.

j. For U.S. Census Bureau, Chief Information Officer, 4600 Silver Hill Road, Suitland, MD 20746.

k. For Bureau of Industry and Security, Chief Information Officer, 1401 Constitution Avenue NW., Washington, DC 20230.

l. For International Trade Administration, Chief Information Officer, 1401 Constitution Avenue NW., Washington, DC 20230.

m. For National Institute of Standards and Technology, Chief Information Officer, 100 Bureau Drive, Gaithersburg, MD 20899.

n. For National Telecommunications and Information Administration, Chief Information Officer, 1401 Constitution Avenue NW., Washington, DC 20230.

o. For National Oceanic and Atmospheric Administration, Chief Information Officer, 1305 East-West Highway, SSMC3, Silver Spring, MD 20910.

p. For U.S. Patent and Trademark Office, Chief Information Officer, 600 Dulany Street, Madison Building, Alexandria, VA 22314.

q. For Office of Inspector General, Chief Information Officer, Chief Information Officer, 1401 Constitution Avenue NW., Washington, DC 20230.

r. For National Technical Information Service, Office of the Chief Information Officer, Security Division, 5301 Shawnee Road., Alexandria, VA 22312.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Employees, contractors, and other affiliates requiring access to Department of Commerce electronic (including PKI-authenticated) and physical assets.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records may include the individual's name; organization; work telephone number; cellular telephone number; home telephone number, work email; Federal agency Smart Card Number (FASC-N); social security number; employee number; status as an employee, contractor or other affiliation with

the Department of Commerce; PIN number (encrypted); sign-in/out, badge-in/out, time-in/out, log-in/out data; computer transaction data to include, but not limited to, key stroke monitoring; IP address of access; logs of internet activity and records on the authentication of the access request; key fob identifier; token identifier; Personal Identity Verification (PIV) Card identifier; computer access login name; and any computer generated identifier assigned to a user.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301; 35 U.S.C. 2; the Electronic Signatures in Global and National Commerce Act, Public Law 106-229; 28 U.S.C. 533-535; 44 U.S.C. 1301; Homeland Security Presidential Directive 12 and IRS Publication-1075.

PURPOSES:

Records in this system are used by authorized personnel to improve security for Department of Commerce physical facilities for purposes including: Ensuring process integrity; enabling employees to carry out their lawful and authorized responsibilities; verifying individuals' authorization to access buildings and facilities; creating a record of individuals' access to buildings and facilities; facilitating the issuance and retrieval of visitor and temporary badges; and providing statistical data on building and facility access patterns including electronic and physical sign/badge-in and sign/badge-out data for resource planning and emergency management purposes.

Records may also be used to secure electronic assets; to maintain accountability for issuance and disposition of security access; to maintain an electronic system to facilitate secure on-line communication between Federal automated systems, between Federal employees or contractors, and with the public, using digital signature technologies to authenticate and verify identity; to provide a means of access to electronic assets, desktops, and laptops; and to provide mechanisms for non-repudiation of personal identification and access to electronic systems, including but not limited to human resource, financial, procurement, travel and property systems, as well as systems containing information on intellectual property and other mission critical systems. The system also maintains records relating to the issuance of digital certificates utilizing public key cryptography to employees

and contractors for the transmission of sensitive electronic material that requires protection.

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

1. Records in this system are accessed on a daily basis by authorized personnel to verify individuals' authorized access to buildings and facilities; electronic systems and computers; facilitate the issuance and retrieval of visitor and temporary badges; determine whether administrative action (including disciplinary action) should be taken regarding any employee, contractor, or visitor; and provide statistical data on computer information systems, building and facility access patterns including electronic and physical sign/badge-in and sign/badge-out data for resource planning, emergency management purposes, assuring the security of computer information systems, and implementing Executive Order 13587.

2. In the event that a system of records maintained by the Department to carry out its functions indicates or relates to a violation or potential violation of law or contract, whether civil, criminal or regulatory in nature, and whether arising by general statute or particular program statute or contract, or rule, regulation, or order issued pursuant thereto, or where necessary to protect an interest of the Department, the relevant records in the system of records may be referred, as a routine use, to the appropriate agency, whether Federal, state, local or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute or contract, or rule, regulation or order issued pursuant thereto, or protecting the interest of the Department.

3. A record from this system of records may be disclosed to a Federal, state or local agency maintaining civil, criminal or other relevant enforcement information or other pertinent information, such as current licenses, if necessary to obtain information relevant to a Department decision concerning the assignment, hiring or retention of an individual, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant or other benefit.

4. A record from this system of records may be disclosed to a Federal, state, local, or international agency, in response to its request, in connection with the assignment, hiring or retention of an individual, the issuance of a

security clearance, the reporting of an investigation of an individual, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter.

5. A record from this system of records may be disclosed in the course of presenting evidence to a court, magistrate or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

6. A record in this system of records may be disclosed to a Member of Congress submitting a request involving an individual when the individual has requested assistance from the Member with respect to the subject matter of the record.

7. A record in this system of records may be disclosed to the Office of Management and Budget in connection with the review of private relief legislation as set forth in OMB Circular No. A-19 at any stage of the legislative coordination and clearance process as set forth in that Circular.

8. A record in this system of records may be disclosed to the Department of Justice in connection with determining whether disclosure thereof is required by the Freedom of Information Act (5 U.S.C. 552).

9. A record in this system of records may be disclosed to a contractor of the Department having need for the information in the performance of the contract, but not operating a system of records within the meaning of 5 U.S.C. 552a(m).

10. A record in this system may be transferred to the Office of Personnel Management for personnel research purposes; as a data source for management information; for the production of summary descriptive statistics and analytical studies in support of the function for which the records are collected and maintained; or for related manpower studies.

11. A record from this system of records may be disclosed to the Administrator, General Services, or his designee, during an inspection of records conducted by the General Services Administration as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e. GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

12. A record in this system of records may be disclosed to appropriate agencies, entities and persons when (1) it is suspected or determined that the security or confidentiality of information in the system of records has been compromised; (2) the DOC 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 whether systems or programs (whether maintained by the DOC 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 the DOC's efforts to respond to the suspected or confirmed compromise and to prevent, minimize, or remedy such harm.

13. A record in this system of records may be disclosed to appropriate agencies, entities and persons for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

Not applicable.

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

STORAGE:

Records in this system are on paper and/or in digital or other electronic form. Paper records are stored in secure rooms and storage cabinets and electronic records are stored as electronic/digital media and stored in secure file-servers within controlled environment. Both paper and electronic/digital records are accessed only by authorized personnel.

RETRIEVABILITY:

Records are retrieved by individual's name, employment status, organization and/or security access badge number, or other Department of Commerce identifier. Information may be retrieved from this system of records by automated search based on extant indices and automated capabilities utilized in the normal course of business.

SAFEGUARDS:

Entrance to data centers and support organization offices is restricted to those employees whose work requires them to be there for the system to operate. Identification cards are verified to ensure that records are in areas accessible only to authorized personnel who are properly screened, cleared, and trained. Disclosure of electronic information through remote terminals is restricted through the use of passwords and sign-on protocols that are periodically changed. Reports produced from the remote printers are subject to the same privacy controls as other documents of like sensitivity.

Electronic and digital certificates ensure secure local and remote access and allow only authorized employees, contractor employees, or other affiliated individuals to gain access to federal information assets available through secured systems access.

Access to sensitive records is available only to authorized employees and contractor employees responsible for the management of the system and/or employees of program offices who have a need for such information. Electronic records are password-protected or PKI-protected, consistent with the requirements of the Federal Information Security Management Act (Pub. L. 107-296), and associated OMB policies, standards and guidance from the National Institute of Standards and Technology, and the General Services Administration, all records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. Access is restricted on a “need to know” basis, utilization of PIV Card access, secure VPN for Web access, and locks on doors and approved storage containers. Buildings have security guards and secured doors. Entrances are monitored through electronic surveillance equipment.

RETENTION AND DISPOSAL:

Records are disposed of in accordance with the appropriate records disposition schedule approved by the Archivist of the United States.

SYSTEM MANAGER(S) AND ADDRESS:

System managers are the same as stated in the System Location section above.

NOTIFICATION PROCEDURE:

An individual requesting notification of existence of records on himself or herself should send a signed, written inquiry to the locations listed below. The request letter should be clearly marked, “PRIVACY ACT REQUEST.” The written inquiry must be signed and notarized or submitted with certification of identity under penalty of perjury. Requesters should reasonably specify the record contents being sought.

For records at locations a., g., and i.: Departmental Freedom of Information and Privacy Act Officer, Room A300, U.S. Department of Commerce, 1401 Constitution Avenue NW., Washington, DC 20230.

For records at locations b., c., and j.: U.S. Census Bureau, Freedom of Information and Privacy Act Officer, Room 8H027, 4600 Silver Hill Road, Washington, DC 20233-3700.

For records at locations d. and m.: National Institute of Standards and Technology, Freedom of Information and Privacy Act Officer, Room 1710, 100 Bureau Drive, Gaithersburg, MD 20899.>

For records at locations e., f., and o.: National Oceanic and Atmospheric Administration, Freedom of Information and Privacy Act Officer, Room 9719, SSMC3, 1315 East-West Highway, Silver Spring, MD 20910.

For records at locations h.and p.: U.S. Patent and Trademark Office, Freedom of Information and Privacy Act Officer, 600 Dulany Street, Madison Building, East, Room 10B20, Alexandria, Virginia 22313.

For records at location k.: Bureau of Industry and Security, Freedom of Information and Privacy Act Officer, Room 6622, 1401 Constitution Avenue NW., Washington, DC 20230.

For records at location l.: International Trade Administration, Freedom of Information and Privacy Act Officer, Room 40003, 1401 Constitution Avenue NW., Washington, DC 20230.

For records at location n.: National Telecommunications and Information Administration, Freedom of Information and Privacy Act Officer, Room 4713, 1401 Constitution Avenue NW., Washington, DC 20230.

For records at location q.: Office of Inspector General, Freedom of Information and Privacy Act Officer, Room 7892, 1401 Constitution Avenue NW., Washington, DC 20230.

For records at location r.: National Technical Information Service, Freedom of Information Act Officer, 5301 Shawnee Road, Alexandria, VA 22312.

RECORD ACCESS PROCEDURES:

An individual requesting access to records on himself or herself should send a signed, written inquiry to the same address as stated in the Notification Procedure section above. The request letter should be clearly marked, “PRIVACY ACT REQUEST.” The written inquiry must be signed and notarized or submitted with certification of identity under penalty of perjury. Requesters should specify the record contents being sought.

CONTESTING RECORD PROCEDURES:

An individual requesting corrections or contesting information contained in his or her records must send a signed, written request inquiry to the same address as stated in the Notification Procedure section above. Requesters should reasonable identify the records, specify the information they are contesting and state the corrective action sought and the reasons for the correction with supporting justification showing how the record is incomplete, untimely, inaccurate, or irrelevant.

The Department's rules for access, for contesting contents, and for appealing initial determination by the individual concerned appear in 15 CFR part 4, Appendix B.

RECORD SOURCE CATEGORIES:

The information contained in these records is provided by or verified by: The subject individual of the record, supervisors, other personnel documents, other Department systems, access log records and sensors and non-Federal

sources such as private employers and their agents, along with those authorized by the individuals to furnish information.

SYSTEM EXEMPTIONS FROM CERTAIN PROVISIONS OF THE ACT:

Pursuant to 5 U.S.C. 552a(j)(2), (k)(1), (k)(2), and (k)(5), all information and material in the record which meets the criteria of these subsections are exempted from the notice, access, and contest requirements under 5 U.S.C. 552a(c)3, (d), (e)(1), (e)(4) (G), (H), and (I), and (f) of the agency regulations because of the necessity to exempt this information and material in order to accomplish the law enforcement function of the agency, to prevent disclosure of classified information as required by Executive Order 12958, as amended by Executive Order 13292, to assure the protection of the President, to prevent subjects of investigation from frustrating the investigatory process, to prevent the disclosure of investigative techniques, to fulfill commitments made to protect the confidentiality of information, and to avoid endangering these sources and law enforcement personnel. In a notice of proposed rulemaking, which is published separately in today's Federal Register, the Department of Commerce is proposing to exempt records maintained in this system from certain provisions of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2), (k)(2), and (k)(5).

FEDERAL REGISTER HISTORY:		
81 FR 64127	September 19, 2016	Notice of Amended Privacy Act System of Records
80 FR 68442	December 7, 2015	Final Rule
80 FR 68500	November 5, 2015	Effective Date Notice
80 FR 36967	June 29, 2015	Comment Period Extension Notice
80 FR 26534	May 8, 2015	Notice of Proposed New Privacy Act System of Records