

waived their rights. Notices of appeal transmitted by facsimile will not be accepted as timely filed.

**Dina L. Torres,**

*Management and Program Analyst, Division of Lands and Cadastral Survey.*

[FR Doc. 2024–20048 Filed 9–5–24; 8:45 am]

**BILLING CODE 4331–10–P**

## DEPARTMENT OF THE INTERIOR

### National Park Service

[DOI–2024–0008; PPWOCRADB0/PCU00RP15.R50000]

#### Privacy Act of 1974; System of Records

**AGENCY:** National Park Service, Interior.

**ACTION:** Notice of a new system of records.

**SUMMARY:** Pursuant to the provisions of the Privacy Act of 1974, as amended, the Department of the Interior (DOI) is issuing a public notice of its intent to create the National Park Service (NPS) Privacy Act system of records, INTERIOR/NPS–35, Cultural Resource Applications System. The system provides the NPS Cultural Resources, Partnerships, and Science (CRPS) Directorate program managers the information needed to make informed cultural resources management decisions. This newly established system will be included in DOI's inventory of record systems.

**DATES:** This new system will be effective upon publication. New routine uses will be effective October 7, 2024. Submit comments on or before October 7, 2024.

**ADDRESSES:** You may send comments identified by docket number [DOI–2024–0008] by any of the following methods:

- *Federal eRulemaking Portal:* <https://www.regulations.gov>. Follow the instructions for sending comments.
  - *Email:* DOI\_Privacy@ios.doi.gov.
- Include docket number [DOI–2024–0008] in the subject line of the message.
- *U.S. Mail or Hand-Delivery:* Teri Barnett, Departmental Privacy Officer, U.S. Department of the Interior, 1849 C Street NW, Room 7112, Washington, DC 20240.

*Instructions:* All submissions received must include the agency name and docket number [DOI–2024–0008]. All comments received will be posted without change to <https://www.regulations.gov>, including any personal information provided.

*Docket:* For access to the docket to read background documents or comments received, go to <https://www.regulations.gov>.

#### FOR FURTHER INFORMATION CONTACT:

Felix Uribe, Associate Privacy Officer, National Park Service, U.S. Department of the Interior, 12201 Sunrise Valley Drive, Reston, VA 20192, [nps\\_privacy@nps.gov](mailto:nps_privacy@nps.gov) or 202–354–6925.

#### SUPPLEMENTARY INFORMATION:

##### I. Background

The CRPS Directorate consists of various applications that support programs under an Associate Director, including the Technical Preservation Services (TPS) Office, National Register of Historic Places and National Historic Landmarks Programs (NR/NHL), Park Archeology Program, Cultural Landscapes, Historic and Prehistoric Structures, and State, Tribal, Local Governments Program, and Tribal Relations and American Cultures. The INTERIOR/NPS–35, Cultural Resource Applications System, system of records provides the NPS CRPS Directorate program managers the ability to centrally manage processes from several program areas. The system helps NPS track, manage, comment and report on grant applications; manage and report on National Register resources in an effective and timely manner; track the processing of applications for Federal income tax incentives for historic preservation; manage NPS's official inventory of cultural resource sites in parks; provide Historic Preservation Offices the ability to report program and financial activities; provide the Native American Graves Protection and Repatriation Act (NAGPRA) Program the ability to track and process data related areas of program work; handle submission, collection, reviewing of the application process and track its progress; create reports, and provide audit documentation; and comply with legal and regulatory requirements for cataloging and reporting on cultural resources and historic properties. To the extent permitted by law, information may be shared with Federal, State, local, Tribal agencies, members of the public, and organizations as authorized and compatible with the purpose of this system, or when proper and necessary, consistent with the routine uses set forth in this system of records notice (SORN).

##### II. Privacy Act

The Privacy Act of 1974, as amended, embodies fair information practice principles in a statutory framework governing how Federal agencies collect, maintain, use, and disseminate individuals' records. The Privacy Act applies to records about individuals that are maintained in a "system of records." A "system of records" is a group of any

records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The Privacy Act defines an individual as a United States citizen or lawful permanent resident. Individuals may request access to their own records that are maintained in a system of records in the possession or under the control of DOI by complying with DOI Privacy Act regulations at 43 CFR part 2, subpart K, and following the procedures outlined in the Records Access, Contesting Record, and Notification Procedures sections of this notice.

The Privacy Act requires each agency to publish in the **Federal Register** a description denoting the existence and character of each system of records that the agency maintains, and the routine uses of each system. The INTERIOR/NPS–35, Cultural Resource Applications System, SORN is published in its entirety below. In accordance with 5 U.S.C. 552a(r), DOI has provided a report of this system of records to the Office of Management and Budget and to Congress.

##### III. Public Participation

You should be aware your entire comment including your personally identifiable information, such as your address, phone number, email address, or any other personal information in your comment, may be made publicly available at any time. While you may request to withhold your personally identifiable information from public review, we cannot guarantee we will be able to do so.

#### SYSTEM NAME AND NUMBER:

INTERIOR/NPS–35, Cultural Resource Applications System.

#### SECURITY CLASSIFICATION:

Unclassified.

#### SYSTEM LOCATION:

Cultural Resources, Partnerships, and Science Directorate, National Park Service, U.S. Department of the Interior, 1849 C Street NW, Room 3316, Washington, DC 20240.

#### SYSTEM MANAGER(S):

Associate Director, Cultural Resources, Partnerships, and Science Directorate, National Park Service, U.S. Department of the Interior, 1849 C Street NW, Room 7518, Washington, DC 20240.

#### AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Archeological Resources Protection Act, 16 U.S.C. 470aa–470mm;

Archeological and Historic Preservation Act, 54 U.S.C. 312501–312508; Protection of Archeological Resources, 43 CFR part 7; Protection of Historic Properties, 36 CFR part 800; National Historic Preservation Act (NHPA), 54 U.S.C. 300101 *et seq.*; National Park Service and Related Programs, 54 U.S.C., section 106 of the National Historic Preservation Act, 54 U.S.C. 306108, section 304 of the National Historic Preservation Act, 54 U.S.C. 307103, section 110 of the National Historic Preservation Act, 54 U.S.C. 306101 *et seq.*; National Historic Landmarks Program, 54 U.S.C. 302102–302108; National Register of Historic Places, 36 CFR part 60; Determinations of Eligibility for Inclusion in the National Register of Historic Places, 36 CFR part 63; National Historic Landmarks Program, 36 CFR part 65; National Park Service Centennial Act, Public Law 114–289 (Dec. 16, 2016); Internal Revenue Code (IRC), 26 U.S.C.; Rehabilitation Credit, 26 U.S.C. 47; Charitable, etc., Contributions and Gifts, 26 U.S.C. 170; Identifying Numbers, 26 U.S.C. 6109; Department of the Interior Regulations, Historic Preservation Certifications Under the Internal Revenue Code, 36 CFR part 67; and African American Civil Rights Network Act of 2017, Public Law 115–104 (Jan. 8, 2018).

**PURPOSE(S) OF THE SYSTEM:**

The purpose of the system is to provide NPS CRPS Directorate program managers the information needed to make informed cultural resources management decisions. The system is used to track the receipt and processing of applications for NPS certification for Federal income tax incentives for historic preservation, track and process grant applications and results, and comply with legal and regulatory requirements for cataloging and reporting on cultural resources and historic properties.

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:**

Individuals covered by the system include NPS employees, Federal contractors, members of the public to include applicants, volunteers, interns, Tribal Historic Preservation Office staff, State Historic Preservation Office staff, and non-profit organization contractors who are associated with grants or projects on National Register or other historic preservation properties or under contracts or agreements with NPS or another Federal agency. This system contains records concerning corporations and other business entities, which are not subject to the Privacy Act.

However, records pertaining to individuals acting on behalf of corporations and other business entities may reflect personal information that may be maintained in this system of records.

**CATEGORIES OF RECORDS IN THE SYSTEM:**

Records covered by the system include:

(1) National Register & Landmarks Application Records. Information in the records include associated persons, events, and/or cultural significance, address, site ownership, and point of contact information, identification of persons or organizations associated to the site, *e.g.*, architect, builder.

(2) Applications for Federal Income Tax Incentives for Historic Preservation. Information in the records include building name and address, owner name, home mailing address, personal email, home phone number, and Social Security number (SSN) or Tax Identification Number (TIN), and associated tax benefit; name, email, and phone number of State, Tribal, or local historic preservation office contact, reference identifier for NRIS–NHL, NPS Reviewer comments, appeal number, project number, dates, and actions such as lack of payment, denials, late or second notices.

Records may include but are not limited to: name, SSN, Tribal Identification Number, other identification numbers, home address, home telephone number, personal cell phone number, personal email address, group affiliation, employment information, financial information, information related to grants and awards, NPS system-assigned project number, and other information as needed to support the system.

**RECORD SOURCE CATEGORIES:**

Records are collected directly from the applicant or owner/agent for the project or property using standard application forms.

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

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DOI as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To the Department of Justice (DOJ), including Offices of the U.S. Attorneys, or other Federal agency conducting litigation or in proceedings before any court, adjudicative, or administrative

body, when it is relevant or necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

(1) DOI or any component of DOI;

(2) Any other Federal agency appearing before the Office of Hearings and Appeals;

(3) Any DOI employee or former employee acting in his or her official capacity;

(4) Any DOI employee or former employee acting in his or her individual capacity when DOI or DOJ has agreed to represent that employee or pay for private representation of the employee; or

(5) The United States Government or any agency thereof, when DOJ determines that DOI is likely to be affected by the proceeding.

B. To a congressional office when requesting information on behalf of, and at the request of, the individual who is the subject of the record.

C. To the Executive Office of the President in response to an inquiry from that office made at the request of the subject of a record or a third party on that person's behalf, or for a purpose compatible with the reason for which the records are collected or maintained.

D. To any criminal, civil, or regulatory law enforcement authority (whether Federal, State, territorial, local, Tribal, or foreign) when a record, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature, and the disclosure is compatible with the purpose for which the records were compiled.

E. To an official of another Federal agency to provide information needed in the performance of official duties related to reconciling or reconstructing data files or to enable that agency to respond to an inquiry by the individual to whom the record pertains.

F. To Federal, State, territorial, local, Tribal, or foreign agencies that have requested information relevant or necessary to the hiring, firing or retention of an employee or contractor, or the issuance of a security clearance, license, contract, grant or other benefit, when the disclosure is compatible with the purpose for which the records were compiled.

G. To representatives of the National Archives and Records Administration (NARA) to conduct records management inspections under the authority of 44 U.S.C. 2904 and 2906.

H. To State, territorial, and local governments and Tribal organizations to provide information needed in response to court order and/or discovery

purposes related to litigation, when the disclosure is compatible with the purpose for which the records were compiled.

I. To an expert, consultant, grantee, shared service provider, or contractor (including employees of the contractor) of DOI that performs services requiring access to these records on DOI's behalf to carry out the purposes of the system.

J. To appropriate agencies, entities, and persons when:

(1) DOI suspects or has confirmed that there has been a breach of the system of records.

(2) DOI has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOI (including its information systems, programs, and operations), the Federal Government, or national security; and

(3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DOI's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

K. To another Federal agency or Federal entity, when DOI determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in:

(1) responding to a suspected or confirmed breach; or

(2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

L. To the Office of Management and Budget (OMB) during the coordination and clearance process in connection with legislative affairs as mandated by OMB Circular A-19.

M. To the Department of the Treasury to recover debts owed to the United States.

N. To the news media and the public, with the approval of the Public Affairs Officer in consultation with counsel and the Senior Agency Official for Privacy, where there exists a legitimate public interest in the disclosure of the information, except to the extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

O. To the Internal Revenue Service and State Historic Preservation Offices for the purpose of processing applications for NPS certification for Federal income tax incentives for historic preservation and to meet

regulatory requirements for administration of the system.

**POLICIES AND PRACTICES FOR STORAGE OF RECORDS:**

Paper records are stored in locked file cabinets in locked offices. Electric records are stored on file servers which is hosted by the NPS data center.

**POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:**

Records in this system are retrieved by various fields including the first name, last name of an individual, name of a historic property, property location, and NPS system-assigned project number.

**POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:**

Records in this system are retained in accordance with the NPS Records Schedule, Resource Management and Lands, which has been approved by the National Archives and Records Administration (NARA) (Job No. NI-79-08-01), for records documenting the acquisition, planning, management, and protection of lands and natural and cultural resources under the stewardship of NPS. The disposition for records in the system is permanent and records are transferred to permanent special media and electronic records along with any finding aids or descriptive information (including linkage to the original file), and related documentation by calendar year to the National Archives when 3 years old. Digital records will be transferred according to standards applicable at the time. All other permanent records are transferred to NARA 7 years after closure.

**ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:**

The records contained in this system are safeguarded in accordance with 43 CFR 2.226 and other applicable security and privacy rules and policies. Paper records are maintained in locked file cabinets in locked offices under the control of authorized personnel. Computer servers on which electronic records are stored and located are in secured DOI controlled areas with physical, technical, and administrative levels of security to prevent unauthorized access to the DOI network and information assets.

Computerized records systems follow the National Institute of Standards and Technology privacy and security standards as developed to comply with the Privacy Act of 1974, as amended, 5 U.S.C. 552a; Paperwork Reduction Act of 1995, 44 U.S.C. 3501 *et seq.*; Federal Information Security Modernization Act

of 2014, 44 U.S.C. 3551 *et seq.*; and the Federal Information Processing Standards 199: Standards for Security Categorization of Federal Information and Information Systems. Security controls include user identification, passwords, database permissions, encryption, firewalls, audit logs, and network system security monitoring, and software controls.

The system is accessed by NPS authorized employees, contractors, and volunteers (collectively, NPS users) using the Personal Identity Verification (PIV) credentials and DOI Active Directory for authentication and role/permission management. NPS users must complete a background check and are required to sign the DOI Rules of Behavior and must complete security and privacy training prior to accessing the DOI computer system or network. A Privacy Impact Assessment was conducted on the Cultural Resource Applications System to ensure that Privacy Act requirements are met, and appropriate privacy controls were implemented to safeguard the personally identifiable information contained in the system.

Government user access will be authorized according to their role and permissions using a formal process for ensuring least privilege access is maintained before their accounts are created through the Role Based Access Control (RBAC) system. Government users will authenticate to RBAC using the applicable agency identity provider (*e.g.*, Active Directory Federated Services for DOI) and their issued PIV card. The system uses audit logs to protect against unauthorized access, changes or use of data.

Non-NPS users, including users from other Federal agencies, State governments, local governments, Tribal organizations, universities, or the general public, must first obtain approval from program managers and register to have a user account created. The system user management tools provide multifactor authentication using a valid email account and a temporary encrypted account confirmation code. The system can be accessed through NPS public and internal network portals. Access to data is restricted to authorized personnel who require access to perform their official duties. Access to administrative functions is strictly controlled.

For all users, the permissions will determine what function the user may execute in the system and define what records the user can enter, edit, read, or delete. System administrators are required to view usernames and permissions for troubleshooting and for

system maintenance purposes. NPS employees and contractors with privileged accounts will be subject to routine auditing to ensure compliance with policies and procedures for managing data confidentiality and integrity. System administrators periodically review audit logs to prevent unauthorized monitoring for all users based on authorized and assigned roles and permissions.

#### RECORD ACCESS PROCEDURES:

An individual requesting access to their records should send a written inquiry to the System Manager identified above. DOI forms and instructions for submitting a Privacy Act request may be obtained from the DOI Privacy Act Requests website at <https://www.doi.gov/privacy/privacy-act-requests>. The request must include a general description of the records sought and the requester's full name, current address, and sufficient identifying information such as date of birth or other information required for verification of the requester's identity. The request must be signed and dated and be either notarized or submitted under penalty of perjury in accordance with 28 U.S.C. 1746. Requests submitted by mail must be clearly marked "PRIVACY ACT REQUEST FOR ACCESS." on both the envelope and letter. A request for access must meet the requirements of 43 CFR 2.238.

#### CONTESTING RECORD PROCEDURES:

An individual requesting amendment of their records should send a written request to the System Manager as identified above. DOI instructions for submitting a request for amendment of records are available on the DOI Privacy Act Requests website at <https://www.doi.gov/privacy/privacy-act-requests>. The request must clearly identify the records for which amendment is being sought, the reasons for requesting the amendment, and the proposed amendment to the record. The request must include the requester's full name, current address, and sufficient identifying information such as date of birth or other information required for verification of the requester's identity. The request must be signed and dated and be either notarized or submitted under penalty of perjury in accordance with 28 U.S.C. 1746. Requests submitted by mail must be clearly marked "PRIVACY ACT REQUEST FOR AMENDMENT" on both the envelope and letter. A request for amendment must meet the requirements of 43 CFR 2.246.

#### NOTIFICATION PROCEDURES:

An individual requesting notification of the existence of records about them should send a written inquiry to the System Manager as identified above. DOI instructions for submitting a request for notification are available on the DOI Privacy Act Requests website at <https://www.doi.gov/privacy/privacy-act-requests>. The request must include a general description of the records and the requester's full name, current address, and sufficient identifying information such as date of birth or other information required for verification of the requester's identity. The request must be signed and dated and be either notarized or submitted under penalty of perjury in accordance with 28 U.S.C. 1746. Requests submitted by mail must be clearly marked "PRIVACY ACT INQUIRY" on both the envelope and letter. A request for notification must meet the requirements of 43 CFR 2.235.

#### EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

#### HISTORY:

None.

#### Teri Barnett,

*Departmental Privacy Officer, U.S. Department of the Interior.*

[FR Doc. 2024-20104 Filed 9-5-24; 8:45 am]

BILLING CODE 4312-52-P

#### INTERNATIONAL TRADE COMMISSION

[Investigation No. 337-TA-1343]

#### Certain Video Processing Devices and Components Thereof; Notice of a Commission Determination To Review in Part a Final Initial Determination Finding No Violation of Section 337 and, on Review, To Affirm the Finding of No Violation; Termination of the Investigation

**AGENCY:** U.S. International Trade Commission.

**ACTION:** Notice.

**SUMMARY:** Notice is hereby given that the U.S. International Trade Commission has determined to review in part a final initial determination ("ID") issued by the presiding administrative law judge ("ALJ") on May 29, 2024, finding no violation of section 337 in the above-referenced investigation and, on review, to affirm the finding of no violation. The investigation is terminated.

**FOR FURTHER INFORMATION CONTACT:** Michael Liberman, Esq., Office of the

General Counsel, U.S. International Trade Commission, 500 E Street SW, Washington, DC 20436, telephone (202) 205-2392. Copies of non-confidential documents filed in connection with this investigation may be viewed on the Commission's electronic docket (EDIS) at <https://edis.usitc.gov>. For help accessing EDIS, please email [EDIS3Help@usitc.gov](mailto:EDIS3Help@usitc.gov). General information concerning the Commission may also be obtained by accessing its internet server at <https://www.usitc.gov>. Hearing-impaired persons are advised that information on this matter can be obtained by contacting the Commission's TDD terminal on (202) 205-1810.

**SUPPLEMENTARY INFORMATION:** The Commission instituted this investigation on November 29, 2022, based on a complaint filed on behalf of DivX, LLC ("DivX") of San Diego, CA. 87 FR 73328 (Nov. 29, 2022). The complaint alleges violations of section 337 of the Tariff Act of 1930, as amended, 19 U.S.C. 1337, in the importation into the United States, the sale for importation, or the sale within the United States after importation of certain video processing devices and components thereof by reason of infringement of claims 1-7 and 10-16 of U.S. Patent No. 11,050,808 ("the '808 patent"); claims 1, 2, and 4 of U.S. Patent No. 8,832,297 ("the '297 patent"); claims 29-32 of U.S. Patent No. 7,295,673 ("the '673 patent"); claims 1-11 of U.S. Patent No. 10,225,588 ("the '588 patent"); and claims 11-13 and 15-17 of U.S. Patent No. 11,102,553 ("the '553 patent"). *Id.* The complaint further alleges that a domestic industry exists. *Id.* at 62568. The Commission's notice of investigation named Amazon.com, Inc. ("Amazon") of Seattle, WA and VIZIO, Inc. ("VIZIO") of Irvine, CA as respondents. *Id.* The Office of Unfair Import Investigations is not a party in this investigation. *Id.*

DivX's allegations with respect to the '808 patent were terminated as to respondent Amazon. *See* Order No. 30 (Aug. 21, 2023), *unreviewed by Comm'n Notice* (Sept. 18, 2023).

Respondent VIZIO was terminated from the investigation. *See* Order No. 33 (Sept. 11, 2023), *unreviewed by Comm'n Notice* (Oct. 11, 2023).

DivX's allegations were terminated with respect to claims 12, 13, 15, and 16 of the '553 patent; claims 3, 4, 8, 9, and 10 of the '588 patent; claim 4 of the '297 patent; and claim 31 of the '673 patent. *See* Order No. 53 (Dec. 20, 2023), *unreviewed by Comm'n Notice* (Jan. 9, 2024).

On May 29, 2024, the ALJ issued a final ID on violation of section 337 and