unclassified and classified networks will also follow the same retention schedule.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

USCG safeguards NOAD data in accordance with applicable laws, rules, and policies. All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. These safeguards include role-based access provisions, restricting access to authorized personnel who have a need-to-know, using locks, and password-protection identification features. USCG file areas are locked after normal duty hours and the facilities are protected from the outside by security personnel. In addition, the system manager has the capability to maintain system back-ups for the purpose of supporting continuity of operations and the discrete need to isolate and copy specific data access transactions for the purpose of conducting security incident investigations. All communication links with the USCG datacenter are encrypted. The databases are Certified with the USCG datacenter are encrypted. The databases are Certified

RECORD ACCESS PROCEDURES:

The Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act, and those of the Judicial Redress Act if applicable, because it is a law enforcement system. However, DHS/USCG will consider individual requests to determine whether or not information may be released. Thus, individuals seeking access to and notification of any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the Chief Privacy Officer and Headquarters or USCG’s FOIA Officer, whose contact information can be found at http://www.dhs.gov/foia under “Contacts Information.” If an individual believes that person, or his or her agent, seeks access to or amendment of such information.

The Privacy Act, however, requires DHS to maintain an accounting of the disclosures made pursuant to all routines uses. Disclosing the fact that a law enforcement or intelligence agency has sought particular records may affect ongoing law enforcement activities. The Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(k)(2), exempted this system from the following provisions of the Privacy Act: Sections (c)(3), (e)(8), and (g) of the Privacy Act of 1974, as amended, as necessary and appropriate to protect this information. Further, DHS has exempted section (c)(3) of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(k)(2) as is necessary and appropriate to protect this information.

SAFEGUARDS:

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

USCG safeguards NOAD data in accordance with applicable laws, rules, and policies. All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. These safeguards include role-based access provisions, restricting access to authorized personnel who have a need-to-know, using locks, and password-protection identification features. USCG file areas are locked after normal duty hours and the facilities are protected from the outside by security personnel. In addition, the system manager has the capability to maintain system back-ups for the purpose of supporting continuity of operations and the discrete need to isolate and copy specific data access transactions for the purpose of conducting security incident investigations. All communication links with the USCG datacenter are encrypted. The databases are Certified

RECORD ACCESS PROCEDURES:

The Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act, and those of the Judicial Redress Act if applicable, because it is a law enforcement system. However, DHS/USCG will consider individual requests to determine whether or not information may be released. Thus, individuals seeking access to and notification of any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the Chief Privacy Officer and Headquarters or USCG’s FOIA Officer, whose contact information can be found at http://www.dhs.gov/foia under “Contacts Information.” If an individual believes that person, or his or her agent, seeks access to or amendment of such information.

The Privacy Act, however, requires DHS to maintain an accounting of the disclosures made pursuant to all routines uses. Disclosing the fact that a law enforcement or intelligence agency has sought particular records may affect ongoing law enforcement activities. The Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(k)(2), exempted this system from the following provisions of the Privacy Act: Sections (c)(3), (e)(8), and (g) of the Privacy Act of 1974, as amended, as necessary and appropriate to protect this information. Further, DHS has exempted section (c)(3) of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(k)(2) as is necessary and appropriate to protect this information.

SAFEGUARDS:

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

USCG safeguards NOAD data in accordance with applicable laws, rules, and policies. All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. These safeguards include role-based access provisions, restricting access to authorized personnel who have a need-to-know, using locks, and password-protection identification features. USCG file areas are locked after normal duty hours and the facilities are protected from the outside by security personnel. In addition, the system manager has the capability to maintain system back-ups for the purpose of supporting continuity of operations and the discrete need to isolate and copy specific data access transactions for the purpose of conducting security incident investigations. All communication links with the USCG datacenter are encrypted. The databases are Certified

RECORD ACCESS PROCEDURES:

The Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act, and those of the Judicial Redress Act if applicable, because it is a law enforcement system. However, DHS/USCG will consider individual requests to determine whether or not information may be released. Thus, individuals seeking access to and notification of any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the Chief Privacy Officer and Headquarters or USCG’s FOIA Officer, whose contact information can be found at http://www.dhs.gov/foia under “Contacts Information.” If an individual believes that person, or his or her agent, seeks access to or amendment of such information.

The Privacy Act, however, requires DHS to maintain an accounting of the disclosures made pursuant to all routines uses. Disclosing the fact that a law enforcement or intelligence agency has sought particular records may affect ongoing law enforcement activities. The Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(k)(2), exempted this system from the following provisions of the Privacy Act: Sections (c)(3), (e)(8), and (g) of the Privacy Act of 1974, as amended, as necessary and appropriate to protect this information. Further, DHS has exempted section (c)(3) of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(k)(2) as is necessary and appropriate to protect this information.

SAFEGUARDS:

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

USCG safeguards NOAD data in accordance with applicable laws, rules, and policies. All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. These safeguards include role-based access provisions, restricting access to authorized personnel who have a need-to-know, using locks, and password-protection identification features. USCG file areas are locked after normal duty hours and the facilities are protected from the outside by security personnel. In addition, the system manager has the capability to maintain system back-ups for the purpose of supporting continuity of operations and the discrete need to isolate and copy specific data access transactions for the purpose of conducting security incident investigations. All communication links with the USCG datacenter are encrypted. The databases are Certified

RECORD ACCESS PROCEDURES:

The Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act, and those of the Judicial Redress Act if applicable, because it is a law enforcement system. However, DHS/USCG will consider individual requests to determine whether or not information may be released. Thus, individuals seeking access to and notification of any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the Chief Privacy Officer and Headquarters or USCG’s FOIA Officer, whose contact information can be found at http://www.dhs.gov/foia under “Contacts Information.” If an individual believes that person, or his or her agent, seeks access to or amendment of such information.

The Privacy Act, however, requires DHS to maintain an accounting of the disclosures made pursuant to all routines uses. Disclosing the fact that a law enforcement or intelligence agency has sought particular records may affect ongoing law enforcement activities. The Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(k)(2), exempted this system from the following provisions of the Privacy Act: Sections (c)(3), (e)(8), and (g) of the Privacy Act of 1974, as amended, as necessary and appropriate to protect this information. Further, DHS has exempted section (c)(3) of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(k)(2) as is necessary and appropriate to protect this information.

SAFEGUARDS:

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

USCG safeguards NOAD data in accordance with applicable laws, rules, and policies. All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. These safeguards include role-based access provisions, restricting access to authorized personnel who have a need-to-know, using locks, and password-protection identification features. USCG file areas are locked after normal duty hours and the facilities are protected from the outside by security personnel. In addition, the system manager has the capability to maintain system back-ups for the purpose of supporting continuity of operations and the discrete need to isolate and copy specific data access transactions for the purpose of conducting security incident investigations. All communication links with the USCG datacenter are encrypted. The databases are Certified
listed fish, wildlife, or plant species. All species included in the incidental take permit would receive assurances under our “No Surprises” regulations (50 CFR 17.22(b)(5) and 17.32(b)(5)).

The applicant has applied for a permit for incidental take of the California tiger salamander and California red-legged frog. The potential taking would occur as a result of activities associated with the construction of the farm labor camp in suitable habitat for the covered species.

Our Preliminary Determination

The Service has made a preliminary determination that issuance of the permit is neither a major Federal action that will significantly affect the quality of the human environment within the meaning of section 102(2)(C) of the National Environmental Policy Act (42 U.S.C. 4321 et seq.; NEPA), nor will it individually or cumulatively have more than a negligible effect on the species covered in the HCP. Therefore, the permit qualifies for a categorical exclusion under NEPA.

Public Comments

If you wish to comment on the permit application, plan, and associated documents, you may submit comments by one of the methods in ADDRESSES.

Public Availability of Comments

Before including your address, phone number, email address, or other personal identifying information in your comment, you should be aware that your entire comment, including your personal identifying information, may be made publicly available at any time. While you can ask us in your comment to withhold your personal identifying information from public view, we cannot guarantee that we will be able to do so.

Authority

We provide this notice under section 10 of the Act (16 U.S.C. 1531 et seq.) and NEPA regulations (40 CFR 1506.6).

Dated: July 11, 2017.

Stephen P. Henry,
Field Supervisor, Ventura Fish and Wildlife Office, Ventura, California.

DEPARTMENT OF THE INTERIOR

Bureau of Indian Affairs

[178A2100DD/AAKC001030/ A0A501010.999900 253G]

Indian Gaming: Approval of an Amendment to a Tribal-State Class III Gaming Compact in the State of Arizona

AGENCY: Bureau of Indian Affairs, Interior.

ACTION: Notice.

SUMMARY: The Tohono O’odham Nation of Arizona and State of Arizona negotiated an Agreement to Amend Compact between the Tohono O’odham Nation and the State of Arizona governing Class III gaming; this notice announces approval of the Agreement to Amend Compact.

DATES: This notice takes effect July 17, 2017.

FOR FURTHER INFORMATION CONTACT: Ms. Paula L. Hart, Director, Office of Indian Gaming, Office of the Assistant Secretary—Indian Affairs, Washington, DC 20240, (202) 219–4066.

SUPPLEMENTARY INFORMATION: Section 11 of the Indian Gaming Regulatory Act (IGRA) requires the Secretary of the Interior to publish in the Federal Register notice of approved Tribal-State compacts that are for the purpose of engaging in Class III gaming activities on Indian lands. See Public Law 100–497, 25 U.S.C. 2701 et seq. All Tribal-State Class III compacts, including amendments, are subject to review and approval by the Secretary under 25 CFR 293.4. The Agreement to Amend Compact prohibits gaming in the Geographical Area with the exception of one gaming facility on the West Valley Trust Land, increases the number of Keno games to four within each of the Tribe’s facilities, and allows for the operation of an additional five poker tables within each gaming facility. The Agreement to Amend Compact is approved. See 25 U.S.C. 2710(d)(8)(A).


Michael S. Black,
Acting Assistant Secretary—Indian Affairs.

[FR Doc. 2017–14881 Filed 7–14–17; 8:45 am]
BILLING CODE 4337–15–P