

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

All Department of State network users are given cyber security awareness training which covers the procedures for handling Sensitive but Unclassified (SBU) information, including personally identifiable information (PII). Annual refresher training is mandatory. In addition, all Department OpenNet users are required to take the Foreign Service Institute distance learning course instructing employees on privacy and security requirements, including the rules of behavior for handling PII and the potential consequences if it is handled improperly. Before being granted access to Foreign Service Institute Records, a user must first be granted access to the Department of State computer system.

Department of State employees and contractors may remotely access this system of records using non-Department owned information technology. Such access is subject to approval by the Department's mobile and remote access program and is limited to information maintained in unclassified information systems. Remote access to the Department's information systems is configured in compliance with OMB Circular A-130 multifactor authentication requirements and includes a time-out function.

All Department of State employees and contractors with authorized access to records maintained in this system of records have undergone a thorough background security investigation. Access to the Department of State, its annexes, and posts abroad is controlled by security guards and admission is limited to those individuals possessing a valid identification card or individuals under proper escort. Access to computerized files is password-protected and under the direct supervision of the system manager. The system manager has the capability of printing audit trails of access from the computer media, thereby permitting regular and ad hoc monitoring of computer usage. When it is determined that a user no longer needs access, the user account is disabled.

The safeguards in the following paragraphs apply only to records that are maintained in government-certified cloud systems. All cloud systems that provide IT services and process Department of State information must be specifically authorized by the Department of State Authorizing Official and Senior Agency Official for Privacy.

Information that conforms with Department-specific definitions for Federal Information Security Modernization Act (FISMA) low,

moderate, or high categorization are permissible for cloud usage and must specifically be authorized by the Department's Cloud Program Management Office and the Department of State Authorizing Official. Specific security measures and safeguards will depend on the FISMA categorization of the information in a given cloud system. In accordance with Department policy, systems that process more sensitive information will require more stringent controls and review by Department cybersecurity experts prior to approval. Prior to operation, all Cloud systems must comply with applicable security measures that are outlined in FISMA, FedRAMP, OMB regulations, National Institute of Standards and Technology's (NIST) Special Publications (SP) and Federal Information Processing Standards (FIPS) and Department of State policies and standards.

All data stored in cloud environments categorized above a low FISMA impact risk level must be encrypted at rest and in-transit using a federally-approved encryption mechanism. The encryption keys shall be generated, maintained, and controlled in a Department data center by the Department key management authority. Deviations from these encryption requirements must be approved in writing by the Department of State Authorizing Official. High FISMA impact risk level systems will additionally be subject to continual auditing and monitoring, multifactor authentication mechanism utilizing Public Key Infrastructure (PKI) and NIST 800 53 controls concerning virtualization, servers, storage, and networking, as well as stringent measures to sanitize data from the cloud service once the contract is terminated.

RECORD ACCESS PROCEDURES:

Individuals who wish to gain access to or amend records pertaining to themselves should write to U.S. Department of State; Director, Office of Information Programs and Services; A/GIS/IPS; 2201 C Street NW, Room B-266; Washington, DC 20520. The individual must specify that he or she wishes the Foreign Service Institute Records to be checked. At a minimum, the individual must include: full name (including maiden name, if appropriate) and any other names used; current mailing address and zip code; date and place of birth; notarized signature or statement under penalty of perjury; a brief description of the circumstances that caused the creation of the record (including the city and/or country and the approximate dates) which gives the individual cause to believe that Foreign Service Institute Records include

records pertaining to the individual. Detailed instructions on Department of State procedures for accessing and amending records can be found on the Department's FOIA website at <https://foia.state.gov/Request/Guide.aspx>.

CONTESTING RECORD PROCEDURES:

Individuals who wish to contest record procedures should write to U.S. Department of State; Director, Office of Information Programs and Services; A/GIS/IPS; 2201 C Street NW, Room B-266; Washington, DC 20520.

NOTIFICATION PROCEDURES:

Individuals who have reason to believe that this system of records may contain information pertaining to them may write to U.S. Department of State; Director, Office of Information Programs and Services; A/GIS/IPS; 2201 C Street NW, Room B-266; Washington, DC 20520. The individual must specify that he/she wishes the Foreign Service Institute Records to be checked. At a minimum, the individual must include: full name (including maiden name, if appropriate) and any other names used; current mailing address and zip code; date and place of birth; notarized signature or statement under penalty of perjury; a brief description of the circumstances that caused the creation of the record (including the city and/or country and the approximate dates) which gives the individual cause to believe that Foreign Service Institute of Records include records pertaining to the individual.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

Pursuant to 5 U.S.C. 552a (k)(6) records in this system of records may be exempted from 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H) and (I) and (f).

HISTORY:

Previously published at 71 FR 8882 (February 21, 2006).

Eric F. Stein,

Deputy Assistant Secretary, Global Information Services (A/GIS), Department of State.

[FR Doc. 2023-09813 Filed 5-8-23; 8:45 am]

BILLING CODE 4710-34-P

DEPARTMENT OF STATE

[Public Notice: 12069]

International Security Advisory Board (ISAB) Meeting Notice; Closed Meeting

In accordance with section 10(a)(2) of the Federal Advisory Committee Act, 5 U.S.C. 1009(a)(2), the Department of State announces a meeting of the International Security Advisory Board

(ISAB) to take place on June 05, 2023, at the Department of State, Washington, DC.

Pursuant to section 10(d) of the Federal Advisory Committee Act, 5 U.S.C. 1009(d), and 5 U.S.C. 552b(c)(1), it has been determined that this Board meeting will be closed to the public because the Board will be reviewing and discussing matters properly classified in accordance with E.O. 13526. The purpose of the ISAB is to provide the Department with a continuing source of independent advice on all aspects of arms control, disarmament, nonproliferation, outer space, critical infrastructure, cybersecurity, the national security aspects of associated technologies, international security, and related aspects of public diplomacy. The agenda for this meeting will include classified discussions related to the Board's ongoing studies on current U.S. policy and issues regarding arms control, international security, nuclear proliferation, associated technologies, climate and energy security.

For more information, contact Michelle Dover, Executive Director of the International Security Advisory Board, Department of State, Washington, DC 20520, telephone: (202) 736-4930.

Michelle Dover,

Executive Director, International Security Advisory Board, Department of State.

[FR Doc. 2023-09840 Filed 5-8-23; 8:45 am]

BILLING CODE 4710-35-P

DEPARTMENT OF TRANSPORTATION

Federal Highway Administration

Notice of Final Federal Agency Actions on the Spur 399 Extension Project in Texas

AGENCY: Texas Department of Transportation (TxDOT), Federal Highway Administration (FHWA), U.S. Department of Transportation.

ACTION: Notice of limitation on claims for judicial review of actions by TxDOT and Federal agencies.

SUMMARY: This notice announces actions taken by TxDOT and Federal agencies that are final. The environmental review, consultation, and other actions required by applicable Federal environmental laws for this project are being, or have been, carried out by TxDOT pursuant to an assignment agreement executed by FHWA and TxDOT. These actions grant licenses, permits, and approvals for the Spur 399 Extension Project, from US 75 to US 380 in Collin County, Texas.

DATES: By this notice, TxDOT is advising the public of final agency actions subject to 23 U.S.C. 139(l)(1). A claim seeking judicial review of TxDOT and Federal agency actions on the Spur 399 Extension Project will be barred unless the claim is filed on or before the deadline. For the Spur 399 Extension Project the deadline is October 6, 2023. If the Federal law that authorizes judicial review of a claim provides a time period of less than 150 days for filing such a claim, then that shorter time period still applies.

FOR FURTHER INFORMATION CONTACT:

Patrick Lee, Environmental Affairs Division, Texas Department of Transportation, 125 East 11th Street, Austin, Texas 78701; telephone: (512) 416-2358; email: Patrick.Lee@txdot.gov. TxDOT's normal business hours are 8:00 a.m.–5:00 p.m. (central time), Monday through Friday.

SUPPLEMENTARY INFORMATION: The Spur 399 Extension Project will construct an eight-lane freeway with frontage roads connecting US 75 with US 380. The project will add one travel lane in each direction and an exit ramp within the existing SH 5 corridor extending from the US 75/SH 5/SRT-SH 121 junction to approximately 1,500 feet south of the intersection of FM 546/Harry McKillop Boulevard and SH 5. The project will then extend Spur 399 east on new location crossing Airport Drive/Old Mill Road and continuing further east and south around the southern end of the Airport, then turning north near CR 317 to connect to US 380 east of the Airport. The project is approximately 6.25 miles in length.

The actions by TxDOT and Federal agencies and the laws under which such actions were taken are described in the Final Environmental Impact Statement, Record of Decision (ROD) issued on March 29, 2023, and other documents in the TxDOT project file. The Final Environmental Impact Statement, ROD, and other documents in the TxDOT project file are available by contacting the TxDOT Dallas District Office at 4777 E. Highway 80, Mesquite, TX 75150; telephone: (214) 320-4480.

The environmental review, consultation, and other actions required by applicable Federal environmental laws for the Spur 299 Extension Project are being, or have been, carried-out by TxDOT pursuant to 23 U.S.C. 327 and a Memorandum of Understanding dated December 9, 2019, and executed by FHWA and TxDOT.

Notice is hereby given that TxDOT and Federal agencies have taken final agency actions by issuing licenses,

permits, and approvals for the Spur 399 Extension Project in the State of Texas.

This notice applies to all TxDOT and Federal agency decisions as of the issuance date of this notice and all laws under which such actions were taken, including but not limited to:

1. *General:* National Environmental Policy Act (NEPA) [42 U.S.C. 4321–4351]; Federal-Aid Highway Act [23 U.S.C. 109].

2. *Air:* Clean Air Act [42 U.S.C. 7401–7671(q)].

3. *Land:* Section 4(f) of the Department of Transportation Act of 1966 [49 U.S.C. 303]; Landscaping and Scenic Enhancement (Wildflowers) [23 U.S.C. 319].

4. *Wildlife:* Endangered Species Act [16 U.S.C. 1531–1544 and section 1536], Marine Mammal Protection Act [16 U.S.C. 1361], Fish and Wildlife Coordination Act [16 U.S.C. 661–667(d)], Migratory Bird Treaty Act [16 U.S.C. 703–712].

5. *Historic and Cultural Resources:* Section 106 of the National Historic Preservation Act of 1966, as amended [54 U.S.C. 300101 *et seq.*]; Archeological Resources Protection Act of 1977 [16 U.S.C. 470(aa)–11]; Archeological and Historic Preservation Act [54 U.S.C. 312501 *et seq.*]; Native American Grave Protection and Repatriation Act (NAGPRA) [25 U.S.C. 3001–3013].

6. *Social and Economic:* Civil Rights Act of 1964 [42 U.S.C. 2000(d)–2000(d)(1)]; American Indian Religious Freedom Act [42 U.S.C. 1996]; Farmland Protection Policy Act (FPPA) [7 U.S.C. 4201–4209].

7. *Wetlands and Water Resources:* Clean Water Act [33 U.S.C. 1251–1377] (section 404, section 401, section 319); Land and Water Conservation Fund (LWCF) [16 U.S.C. 4601–4604]; Safe Drinking Water Act (SDWA) [42 U.S.C. 300(f)–300(j)(6)]; Rivers and Harbors Act of 1899 [33 U.S.C. 401–406]; Wild and Scenic Rivers Act [16 U.S.C. 1271–1287]; Emergency Wetlands Resources Act [16 U.S.C. 3921, 3931]; TEA–21 Wetlands Mitigation [23 U.S.C. 103(b)(6)(m), 133(b)(11)]; Flood Disaster Protection Act [42 U.S.C. 4001–4128].

8. *Executive Orders:* E.O. 11990 Protection of Wetlands; E.O. 11988 Floodplain Management; E.O. 12898 Federal Actions to Address Environmental Justice in Minority Populations and Low-Income Populations; E.O. 11593 Protection and Enhancement of Cultural Resources; E.O. 13007 Indian Sacred Sites; E.O. 13287 Preserve America; E.O. 13175 Consultation and Coordination with Indian Tribal Governments; E.O. 11514 Protection and Enhancement of