

Cybersecurity Advisory Committee is committed to ensuring all participants have equal access regardless of disability status. If you require a reasonable accommodation due to a disability to fully participate, please contact Ms. Megan Tsuyi at (202) 594–7374 as soon as possible.

Comments: Members of the public are invited to provide comment on issues that will be considered by the committee as listed in the

SUPPLEMENTARY INFORMATION section below. Associated materials that may be discussed during the meeting will be made available for review at <https://www.cisa.gov/cisa-cybersecurity-advisory-committee-meeting-resources> by Friday, October 4, 2024. Comments must be submitted by 5 p.m. EDT on Friday, October 4, 2024 and must be identified by Docket Number CISA–2024–0003. Comments may be submitted by one of the following methods:

- *Federal eRulemaking Portal:* www.regulations.gov. Please follow the instructions for submitting written comments.

- *Email: CISA CybersecurityAdvisoryCommittee@cisa.dhs.gov.* Include the Docket Number CISA–2024–0003 in the subject line of the email.

Instructions: All submissions received must include the words “Cybersecurity and Infrastructure Security Agency” and the Docket Number for this action. Comments received will be posted without alteration to www.regulations.gov, including any personal information provided. You may wish to review the Privacy & Security notice available via a link on the homepage of www.regulations.gov.

Docket: For access to the docket and comments received by the CISA Cybersecurity Advisory Committee, please go to www.regulations.gov and enter docket number CISA–2024–0003.

A public comment period is scheduled to be held during the meeting from 2:35 p.m. to 2:45 p.m. EDT. Speakers who wish to participate in the public comment period must email CISA_CybersecurityAdvisoryCommittee@cisa.dhs.gov to register. Speakers should limit their comments to three minutes and will speak in order of registration. Please note that the public comment period may end before the time indicated, depending on the number of speakers who register to participate.

FOR FURTHER INFORMATION CONTACT: Megan Tsuyi, 202–594–7374, CISA_CybersecurityAdvisoryCommittee@cisa.dhs.gov.

SUPPLEMENTARY INFORMATION: The CISA Cybersecurity Advisory Committee was established under the National Defense Authorization Act for Fiscal Year 2021, Public Law 116–283. Notice of this meeting is given under Federal Advisory Committee Act (FACA), 5 United States Code, chapter 10. The CISA Cybersecurity Advisory Committee advises the CISA Director on matters related to the development, refinement, and implementation of policies, programs, planning, and training pertaining to the cybersecurity mission of the Agency.

Agenda: The CISA Cybersecurity Advisory Committee will hold a virtual meeting on Friday, October 11, 2024, to discuss current CISA Cybersecurity Advisory Committee activities. The open session will be held from 2:30 p.m. to 4:00 p.m. EDT and will include: public comment, briefings from four CSAC subcommittees, and CSAC member deliberation and vote on recommendations for the Director.

The Committee will also meet in a closed session from 12:30 p.m. to 2:15 p.m. EDT to participate in an operational discussion that will address areas of critical cybersecurity vulnerabilities and priorities for CISA. Government officials will share sensitive information with CSAC members on initiatives and future security requirements for assessing cyber risks to critical infrastructure.

Basis for Closure: In accordance with section 1009(d) of FACA and 5 U.S.C. 552b(c)(9)(B), The Government in the Sunshine Act, it has been determined that certain agenda items require closure, as the premature disclosure of the information that will be discussed would be likely to significantly frustrate implementation of proposed agency actions.

This agenda item addresses areas of CISA’s operations that include critical cybersecurity vulnerabilities and priorities for CISA. Government officials will share sensitive information with CSAC members on initiatives and future security requirements for assessing cyber risks to critical infrastructure.

As the premature disclosure of the information that will be discussed would be likely to significantly frustrate implementation of proposed agency action, this portion of the meeting is required to be closed pursuant to

section 1009(d) of FACA and 5 U.S.C. 552b(c)(9)(B).

Megan M. Tsuyi,

Designated Federal Officer, CISA Cybersecurity Advisory Committee, Cybersecurity and Infrastructure Security Agency, Department of Homeland Security.

[FR Doc. 2024–21527 Filed 9–19–24; 8:45 am]

BILLING CODE 9111–LF–P

DEPARTMENT OF THE INTERIOR

Bureau of Indian Affairs

[245A2100DD/AAKC001030/A0A501010.999900]

Indian Gaming; Extension of Tribal-State Class III Gaming Compact in California

AGENCY: Bureau of Indian Affairs, Interior.

ACTION: Notice.

SUMMARY: This notice announces the extension of the Class III gaming compact between the Alturas Indian Rancheria and the State of California.

DATES: The extension takes effect on September 20, 2024.

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

SUPPLEMENTARY INFORMATION: An extension to an existing Tribal-State Class III gaming compact does not require approval by the Secretary if the extension does not modify any other terms of the compact. 25 CFR 293.5. The Alturas Indian Rancheria and the State of California have reached an agreement to extend the expiration date of their existing Tribal-State Class III gaming compact to December 31, 2024. This publication provides notice of the new expiration date of the compact.

Bryan Newland,

Assistant Secretary—Indian Affairs.

[FR Doc. 2024–21562 Filed 9–19–24; 8:45 am]

BILLING CODE 4337–15–P