# Fiscal Year 2023 Tribal Cybersecurity Grant Program

**Download a PDF copy of this webpage.**

The U.S. Department of Homeland Security (DHS) is providing $18.2 million in Fiscal Year (FY) 2023 under the Tribal Cybersecurity Grant Program (TCGP) to address cybersecurity risks and threats to information systems owned or operated by, or on behalf of, Tribal governments.

## Overview

The goal of the TCGP is to assist Tribal governments with managing and reducing systemic cyber risk. The TCGP enables DHS to provide targeted cybersecurity resources that improve the security of critical infrastructure and resilience of the services that Tribal governments provide to their members. The Cybersecurity and Infrastructure Security Agency (CISA) and Federal Emergency Management Agency (FEMA) are jointly managing the TCGP. CISA will provide cybersecurity programmatic subject-matter expertise by defining goals and objectives, reviewing and approving cybersecurity plans establishing measures of effectiveness, and organizing the Objective Review Panels to review and score applications. FEMA will provide grant administrative oversight by conducting eligibility and completeness reviews as well as issuing and administering the grant awards consistent with all applicable laws, regulations, and policies.

DHS respects the sovereignty and self-determination of Tribal governments and recognizes the intent of Congress to provide flexibility to Tribal governments to meet cybersecurity needs across Indian Country through the TCGP. The framework of the program was made as a result of nation-to-nation consultation with tribal representatives across the country and is intended to support tribal cybersecurity resiliency.

## Objectives

FEMA and CISA developed four overarching objectives for the TCGP based on the consideration of national priorities, frameworks, and the national cyber threat environment:

1. Establish cyber governance and planning;
2. Assess and evaluate systems and capabilities;
3. Implement security protections commensurate with risk; and
4. Build and train a cybersecurity workforce.

Tribal governments must address how they will meet Program Objective 1 in their FY 2023 application. Objectives 2, 3, and 4 are eligible, but are not required, to be addressed in FY 2023 applications. Applicants should refer to *Appendix A: Program Goals and Objectives* in the FY 2023 TCGP Notice of Funding Opportunity (NOFO) for more information on program outcomes required in their application.

## Funding

The funding apportioned for the TCGP for FY 2022 and FY 2023 is $6,000,000 and $12,246,845, respectively. FEMA and CISA combined the funding from both fiscal years into a single TCGP NOFO, which totals $18,246,845.

TCGP utilizes an allocation methodology that establishes four funding categories and divides the $18,246,845 across those four categories. The funding categories allow for applications to be evaluated among applications from similarly populated tribes. Please refer to the FY 2023 TCGP NOFO for more information on the allocation methodology.

## Eligibility

Applicants must meet the definition of “Tribal government” under Section 2220A(a)(7) of the Homeland Security Act of 2002 (codified as amended at 6 U.S.C. § 665g(a)(7). This statute defines “Tribal government” as the recognized governing body of any Indian or Alaska Native Tribe, band, nation, pueblo, village,

community, component band, or component reservation, that is individually identified (including parenthetically) in the most recent list published pursuant to Section 104 of the Federally Recognized Indian Tribe List of 1994 (25 U.S.C. § 5131).

Tribal governments that apply must submit a Cybersecurity Plan, Cybersecurity Planning Committee List, Charter, TCGP Investment Justification (IJ) form, and a Project Worksheet form. These requirements must be fulfilled before a Tribal government may receive TCGP award funding.

Two or more Tribal governments may apply together as a tribal consortium and submit one application for the consortium.

## Funding Guidelines

### Cybersecurity Planning Committee and Cybersecurity Plan Requirements

Each Tribal government is required to establish a Cybersecurity Planning Committee that assists with developing, implementing, and revising the Cybersecurity Plan of the Tribal government, approves the Cybersecurity Plan of the Tribal government, and assists with the determination of effective funding priorities. An existing Tribal Council/Governing Body that includes the participation of (1) a representative from the grants administration office and (2) a Chief Information Officer (CIO), a Chief Information Security Officer (CISO), or an equivalent official to the CIO or CISO with expertise in information technology and systems can be used to meet this requirement and fulfill these duties. If the Tribal government would prefer to establish a separate Cybersecurity Planning Committee, the required members of that committee must include the following: the grants administration office and a designated CIO, CISO, or equivalent official to the CIO or CISO with expertise in IT and systems. Additional members are encouraged but not required.

Cybersecurity Plans are meant to guide implementation of cybersecurity capabilities within the Tribal government. The Cybersecurity Planning Committee is responsible for approving the Cybersecurity Plan and assisting in prioritizing individual projects. Applicants can download the TCGP Cybersecurity Plan Template from Grants.gov. The Cybersecurity Plan Template is an optional tool

for applicants to use to develop and submit their cybersecurity plans with their application to ensure the plan meets all the required statutory elements. CISA is available to provide technical assistance to Tribal governments on Cybersecurity Plan implementation.

CISA considers Cybersecurity Plans to be living, strategic documents. Following the submission of their plan as part of the grant application, Tribal governments may later update their plan. FEMA and CISA are available to provide technical assistance to Tribal governments on developing and updating Cybersecurity Plans.

### Multi-Entity Projects

As an alternative to submitting a single application as a consortium, Tribal governments can group together to address cybersecurity risks and threats to information systems within tribal jurisdictions by submitting multi-entity projects. Each participating Tribal government in the group should include the multi-entity project in their individual IJ submissions with its application. Each Tribal government would, if FEMA and CISA approved and awarded funding for that project, contribute an agreed-upon funding amount to the project.

It is expected that IJs for multi-entity projects will be almost identical. Any differences should be due to alignment with each Tribal government's respective Cybersecurity Plan. Each Tribal government's financial contribution will be funded from its individual TCGP award.

### Cost-Share or Matching Requirements

The matching requirement is waived for the FY 2023 TCGP.

## Application Process

Applying for an award under the TCGP is a multi-step process. In order to apply for a grant award, an applicant must have a Unique Entity Identifier (UEI), Employer Identification Number (EIN), an active System for Award Management (SAM) registration, a Grants.gov account, and an ND Grants account. Applicants are encouraged to register early for SAM and UEI because the registration process can take four weeks or more to complete. Registration should be done in

sufficient time to ensure it does not impact an applicant's ability to meet the required submission deadline.

Eligible applicants should submit their initial application at least one week before the final application submission deadline through the Grants.gov portal at www.grants.gov. Applicants needing Grants.gov support may contact the Grants.gov customer support hotline at (800) 518-4726, which is available 24 hours a day, 7 days a week, except federal holidays. Please refer to *Section D Application and Submission Information* section in the FY 2023 TCGP NOFO for detailed information and instructions.

Eligible applicants will be notified by FEMA within one to two business days and will be asked to proceed with submitting their complete application package in the Non-Disaster (ND) Grants System by the application deadline. Applicants needing technical support with the ND Grants System should contact ndgrants@fema.dhs.gov or (800) 865-4076, Monday through Friday from 9 a.m. – 6 p.m. ET. Completed applications must be submitted no later than 5 p.m. ET on January 10, 2024.

## TCGP Resources

There are a variety of resources available to assist with TCGP applications that address programmatic, technical, and financial questions:

- The FY 2023 TCGP NOFO is located online at grants.gov.
- For additional grants management and application information, please email FEMA-TCGP@fema.dhs.gov.
- For technical assistance related to cybersecurity planning and project development, please email TCGPinfo@cisa.dhs.gov.
- For support regarding financial grants management and budgetary technical assistance, applicants may contact the FEMA Award Administration Help Desk, via e-mail at ASK-GMD@fema.dhs.gov.