FY 2023 Tribal Cybersecurity Grant Program FAQs

Contents

BACKGROUND 3
GENERAL PROGRAM QUESTIONS 3
What is the purpose of the Tribal Cybersecurity Grant Program (TCGP)? 3
How much funding is available? 3
How will funds be allocated? 3
Who is eligible to apply? 3
What is a Tribal Consortium Application? 4
Is the Tribal Cybersecurity Grant Program (TCGP) related to the Tribal Homeland Security Grant Program (THSGP)? 4
Is the Tribal Cybersecurity Grant Program (TCGP) related to the State and Local Cybersecurity Grant Program (SLCGP)? 4
When will Tribal governments receive funding? 4
What is the goal of the program and its corresponding objectives? 4
What are the required programmatic conditions of receiving a TCGP grant? 5
Are there services that recipients are required to utilize? 5
How often should the Nationwide Cybersecurity Review (NCSR) be completed? 5
When are TCGP key dates? 5
How long is the period of performance (POP)? 5
How will proposed projects be evaluated? 6
Are there any Cybersecurity Plan examples or templates? 6
COST SHARE 7
Is there a cost share requirement for the TCGP? 7
MULTI-ENTITY PROJECTS 7
What are multi-entity projects and who can apply? 7
What are the requirements for multi-entity projects? 7
Do multi-entity projects have to be approved by the Cybersecurity Planning Committee of each tribe? 7
How does the process for multi-entity projects work? 7
What must be submitted for multi-entity projects? 7
CYBERSECURITY BEST PRACTICES 8
Are there specific best practices that Tribal governments should adopt? 8
ELIGIBLE EXPENSES 8

How can the grant funds be used? 8
Can personnel be hired with grant funds? 9
What equipment or software should be purchased? 9
CYBERSECURITY PLANNING COMMITTEE 9
What are the Cybersecurity Planning Committee membership requirements? 9
Can existing committees be used? 9
What are the responsibilities of the planning committee? 9
What is the Cybersecurity Planning Committee Charter? 10
How should planning committees prioritize individual projects? 10
CYBERSECURITY PLANS 10
Who is required to submit a Cybersecurity Plan? 10
Who must approve the Cybersecurity Plan before it is submitted to DHS? 10
Can I revise my Cybersecurity Plan? 10
Are there specific requirements for the Cybersecurity Plan? 11
Is DHS able to provide technical assistance to help with Cybersecurity Plan revision? 11
Can funds be used to enhance existing efforts? 11
Can existing plans be used? 11
What will DHS do with the Cybersecurity Plan? 11
Is there a template or guidance for the Cybersecurity Plan? 11
ADDITIONAL INFORMATION 12
Where can I go for more information? 12
What other resources are available to address programmatic, technical, and financial questions? 12

BACKGROUND

As part of the Bipartisan Infrastructure Law, also known as the Infrastructure Investment and Jobs Act (IIJA), Congress established the Tribal Cybersecurity Grant Program (TCGP) to award grants to Tribal Nations to address cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of Tribal Nations. Through funding from the IIJA, herein referred to as the Bipartisan Infrastructure Law (BIL), the TCGP enables DHS to provide targeted cybersecurity resources for Tribal Nations, thus improving the security of critical infrastructure and improving the resilience of the services Tribal Nations provide to their members.

DHS respects the sovereignty and self-determination of Tribal Nations and recognizes the intent of Congress to provide flexibility to tribes 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.

This Frequently Asked Questions document (FAQ) addresses common questions about the TCGP. Information about the State and Local Cybersecurity Grant Program (SLCGP) is available here.

GENERAL PROGRAM QUESTIONS

What is the purpose of the Tribal Cybersecurity Grant Program (TCGP)?

The TCGP provides funding to federally recognized Tribal Nations to address cybersecurity risks and threats to tribally owned or operated information systems. All requirements and program guidance are established in the Notice of Funding Opportunity (NOFO).

How much funding is available?

The total amount of funds available for FY 2023 is approximately $18.2 million. This amount combines $6 million initially appropriated by Congress for Tribal Nations in FY 2022 and $12.2 million for FY 2023.

How will funds be allocated?

TCGP uses a discretionary allocation methodology that establishes four funding categories and divides the $18.2 million across them. The funding categories allow for applications to be evaluated from among applications from similarly populated Tribal Nations. The following table illustrates the four population levels, number of Tribal Nations, and the corresponding combined funding levels for FY 2022 and FY 2023:

Tribal Population	Number of Tribes[1]	Maximum Allocation of Funding Per Category
100,000 or more	8	$8,109,709
10,000-99,999	33	$5,068,568
1,000-9,999	124	$3,041,141
1-999	392	$2,027,427

Who is eligible to apply?

All 574 federally recognized Tribal governments are eligible to apply. Registering and applying for an award under this program is a multi-step process, therefore early registration is encouraged. Tribal Nations that register and apply must fulfill the requirements and complete the final step in the ND Grants System by 5 p.m. ET on the due date. The FY 2023 requirements that must be fulfilled are:

[1] The number of tribes with a population greater than 1 total 557. The remaining 17 tribes have a represented population of less than 1 per the US Census.gov data collected in 2020.

- Submitting a Cybersecurity Plan;
- Establishing and submitting a Cybersecurity Planning Committee Charter; and
- Establishing a Cybersecurity Planning Committee comprised of the required membership types:
    - An existing Tribal Council/Governing Body that includes 1) a grants administration office representative, and 2) a designated Chief Information Officer (CIO), Chief Information Security Officer (CISO), or equivalent official to the CIO or CISO with expertise in Information Technology (IT) may be used to meet the Committee requirement. This body would also be responsible for fulfilling the duties of the committee.

What is a Tribal Consortium Application?

Multiple Tribal Nations may partner to apply as a tribal consortium. A tribal consortium should only submit one application for the group. The tier chosen for review of a grant application from the Tribal Consortium will be based on the highest populated tribe.

For more information on review process and evaluation criteria of FY 2023 requirements, please refer to Section E: Application Review Information of the NOFO.

Is the Tribal Cybersecurity Grant Program (TCGP) related to the Tribal Homeland Security Grant Program (THSGP)?

No. Although both are DHS programs, the TCGP and the THSGP are different grant programs with different requirements and criteria. However, cybersecurity projects funded by the Tribal Homeland Security Grant Program (THSGP) may be considered for Tribal Cybersecurity Grant Program (TCGP) funding if not duplicative of the THSGP project(s).

Is the Tribal Cybersecurity Grant Program (TCGP) related to the State and Local Cybersecurity Grant Program (SLCGP)?

The TCGP and SLCGP are both funded through the BIL but are separate grant programs. Tribal Nations can apply directly for TCGP funding, whereas tribes are only eligible for SLCGP funding as subrecipients. Tribal Nations applying for funding through SLCGP will have to contact their state or territory's State Administrative Agency (SAA). Tribal Nations can receive funding as a direct recipient through the TCGP and as a subrecipient through the SLCGP. More information on the SLCGP can be found here.

When will Tribal Nations receive funding?

For the FY 2023 application period, awarded Tribal governments will receive funding when they receive their "Notice of Grant Award" in the FEMA Non-Disaster (ND) Grants system, and any applicable funding hold(s) have been lifted.

What is the goal of the program and its corresponding objectives?

The overarching goal of the program is to assist Tribal Nations in managing and reducing systemic cyber risks. To accomplish this, CISA has established four discrete, but interrelated objectives:

- Governance and Planning: Develop and establish appropriate governance structures, by implementing and revising Cybersecurity Plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.
- Assessment and Evaluation: Identify areas for improvement in a Tribal Nation's cybersecurity posture based on continuous testing, evaluation, and structured assessments.

- Mitigation: Implement security protections commensurate with risk (outcomes of Objectives 1 and 2), using the best practices as described in element 5 of the required 13 elements of the cybersecurity plans and those further listed in the NOFO.
- Workforce Development: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with their responsibilities as suggested in the National Initiative for Cybersecurity Education.

What are the required programmatic conditions of receiving a TCGP grant?

For FY 2023, TCGP applicants should satisfy the following programmatic conditions for receiving grant funding:

- Establish a Cybersecurity Planning Committee and accompanying Charter;
- Implement a Cybersecurity Plan, unless the Tribal Nations an existing cybersecurity strategic plan that satisfies the requirements outlined in the NOFO; and
- Submit an Investment Justification (IJ) aligned to Objective 1 (applicants may choose to submit additional IJs for Objectives 2, 3, or 4).

For more information, please refer to Section A.10(b): Objectives of the NOFO.

Are there services that recipients are required to utilize?

All TCGP recipients are required to participate in a limited number of free services by CISA. Please note, participation is not required for submission and approval of a grant but is a post-award requirement.

The post-award required services are:

- CISA Cyber Hygiene Services: Vulnerability Scanning; and
- The Multi-State Information Sharing and Analysis Center (MS-ISAC)'s Nationwide Cybersecurity Review.

All TCGP recipients are strongly encouraged to participate in other memberships. For more information on CISA cybersecurity services, please refer to Appendix F: Required, Encouraged, and Optional Services, Memberships, and Resources in the NOFO. Additional free cyber resources for managing risk and strengthening cybersecurity that can be found on the Cyber Resource Hub.

How often should the Nationwide Cybersecurity Review (NCSR) be completed?

Tribal governments are required to complete the NCSR during the first year of the award period of performance and annually thereafter. In FY 2023, the open reporting period for the NCSR is Oct. 1, 2024 – Feb. 28, 2025.

When are TCGP key dates?

- Sept. 27, 2023: NOFO released
- Sept. 27, 2023: Application Start Date
- Jan. 10, 2024: Applications due to ND Grants System

How long is the period of performance (POP)?

The period of performance for each grant year will be 48 months. Extensions to the period of performance for funded grants are allowed on a case-by-case basis and must be requested through the FEMA Preparedness Officer via the ND Grants System.

How will proposed projects be evaluated?

FY 2023 TCGP applications will be evaluated through a three-part review and selection process:

1. A FEMA HQ Preparedness Officer will review applications to ensure that the applicant meets all eligibility requirements and check submitted applications for completeness.
2. CISA will organize an objective review panel and establish programmatic scoring and the selection process. Subject Matter Experts (SMEs) with cybersecurity and tribal engagement experience will serve as review panelists. Reviewers will evaluate applications, score IJs, and make recommendations for funding within each discretionary tier.
3. FEMA HQ Grants Management Specialists will conduct a financial review of the top scoring investments.

The review panel will score individual IJs against the following criteria:

- Overview Section (5 Points)
    - How well are the activities described, including any activities that include planning, organization, equipment, training and/or exercises?
- Baseline Section (5 Points)
    - How well does the investment identify existing capability levels and address capability gaps?
- Project Management and Milestones Section (10 Points total)
    - Does the budget narrative provide a clear explanation of why funds are needed and the outcomes the recipient wants to achieve? (5 points)
    - Will the investment's projects and activities achieve progress during the grant's period of performance? (5 points)
- Accomplishments and Impact Section (5 Points)
    - Does the outcome(s) demonstrate progress towards building the capability and closing the gap(s) identified in the investment?

Each IJ will be reviewed by no less than two reviewers. Reviewers will use their subject matter expertise to provide a score from 1 to 5 for each question. Investments will be selected for recommendation from the highest score to lowest score within each discretionary tier until available FY 2023 TCGP funding has been exhausted. In the event of a tie, CISA and FEMA will give priority to the Tribal government that submitted the Cybersecurity Plan that more effectively meets program objectives and addresses the 13 required Cybersecurity Plan elements.

For more information on project evaluation criteria, please refer to Section E of the NOFO.

Are there any Cybersecurity Plan examples or templates?

Grants.gov has templates for:

- The TCGP Cybersecurity Plan;
- Investment Justification (IJ); and
- Project Worksheet.

These templates can be found on FY 2023 TCGP on grants.gov.

COST SHARE

Is there a cost share requirement for the TCGP?

Cost share (investment of any non-DHS funding) is waived for all grant recipients of the FY 2023 TCGP.

MULTI-ENTITY PROJECTS

What are multi-entity projects and who can apply?

Multiple eligible tribes (i.e., Tribal Nations) can group together to address cybersecurity risks and threats to their information systems.

Each participating tribe should include the multi-entity project in their individual IJ submissions with their application.

For more information on multi-entity grants, please refer to Section A.10 (c.III): Multi-Entity Projects of the NOFO.

What are the requirements for multi-entity projects?

Each tribe participating in a multi-entity project must submit an individual IJ for the proposed multi-entity project. This IJ must include:

- A description of the overarching multi-entity project;
- The division of responsibilities among the participating Tribal governments;
- The distribution of funding among the participating tribal group members; and
- A description of how the project will help implement the Cybersecurity Plan of each Tribal Nation.

Do multi-entity projects have to be approved by the Cybersecurity Planning Committee of each tribe?

Yes. These projects should be included in the application from each Tribal Nation, approved by the respective Planning Committee and be aligned with each tribe's approved Cybersecurity Plan.

How does the process for multi-entity projects work?

There is no separate funding for multi-entity projects. Instead, they should be considered as group projects where each Tribal government contributes a portion to the overarching effort. Tribal Nations will work collaboratively to define the group project and the roles and responsibilities for each tribe.

- Each Tribal Nation must have a respective Cybersecurity Plan that has been approved by DHS.
- The project must improve or sustain capabilities identified in the respective Cybersecurity Plans for each Tribal Nations.
- The Cybersecurity Planning Committee of each participating Tribal Nation must approve their portion of the group project.

Each Tribal Nation participating in a multi-entity project must submit its own application, including IJs, Cybersecurity Plan and Cybersecurity Planning Committee. All members of the multi-entity project must have an approved Cybersecurity Plan to receive funding for the multi-entity project.

What must be submitted for multi-entity projects?

Each Tribal Nation applicant will be required to submit the following as part of the application package:

- A description of the overarching multi-entity project;
- The other participating Tribal Nations;
- The division of responsibilities among the tribes;
- The distribution of funding from the grant among the tribes that comprise the multi-entity project; and
- How the project will help achieve the goals and objectives of each project members' Cybersecurity Plan.

CYBERSECURITY BEST PRACTICES

Are there specific best practices that Tribal Nations should adopt?

Yes. Cybersecurity Plans must address how the 13 statutorily required elements will be implemented across Tribal governments from a strategic perspective. Adoption is not required immediately, nor by all Tribal Nations. Instead, the Cybersecurity Plan should detail the implementation approach over time and how the following will be consistent with the program goal and objectives.

Tribal governments should consider aligning their projects to the following recommended best practices:

- Implement multi-factor authentication;
- Implement enhanced logging;
- Data encryption for data at rest and in transit;
- End use of unsupported/end of life software and hardware that are accessible from the Internet;
- Prohibit use of known/fixed/default passwords and credentials;
- Ensure the ability to reconstitute systems (backups);
- Actively engage in bidirectional information sharing with CISA in cyber relevant time frames to decrease risk; and
- Migration to the .gov internet domain.

ELIGIBLE EXPENSES

How can the grant funds be used?

Eligible Tribal Nations CAN use grant funds for:

- Implementing or revising the Cybersecurity Plan;
- Paying expenses directly relating to the administration of the grant, which cannot exceed 5% of the amount of the grant award;
- Assisting with allowed activities that address imminent cybersecurity threats confirmed by DHS; and
- Other appropriate activities as noted in the funding notice.

Funds CANNOT be used for:

- Spyware;
- Construction or renovation;
- Payment of a ransom from cyberattacks;

- Recreational or social purposes, or for any purpose that does not address cybersecurity risks or cybersecurity threats on a Tribal Nation's information systems;
- Lobbying or intervention in federal regulatory or adjudicatory proceedings;
- Suing the federal government or any other government entity;
- Acquiring land or constructing, remodeling, or altering buildings or other physical facilities;
- Cybersecurity Insurance; or
- Any purpose that does not address cybersecurity risks or cybersecurity threats on information systems owned or operated by, or on behalf of, the Tribal Nations.

Can personnel be hired with grant funds?

Yes, if aligned to the Cybersecurity Plan. Applicants must address how these functions will be sustained when the funds are no longer available.

What equipment or software should be purchased?

Based on their Cybersecurity Plan, applicants should determine what equipment is most appropriate for their needs to mitigate cybersecurity risks or gaps.

CYBERSECURITY PLANNING COMMITTEE

What are the Cybersecurity Planning Committee membership requirements?

If a Tribal Nations decides to create a new Cybersecurity Planning Committee, it must include representation from each of the following:

- The Tribal Nations;
- The Chief Information Officer (CIO), the Chief Information Security Officer (CISO), or CIO/CISO-equivalent official of the Tribal Nation with IT experience; and
- The Grants Administration office.

Additional members are encouraged, but not required.

Can existing committees be used?

Yes, Tribal Nations can use an existing Tribal Council/Governing Body that includes their CIO, CISO or CIO/CISO-equivalent person with information technology (IT) expertise and grants administration representative.

What are the responsibilities of the planning committee?

The responsibilities of the Cybersecurity Planning Committee include:

- Assisting with the implementation, and revision of the Cybersecurity Plan;
- Approving the Cybersecurity Plan;
- Assisting with the determination of effective funding priorities;
- Coordinating with other committees with the goal of maximizing coordination and reducing duplication of effort; and

- Ensuring investments support closing capability gaps or sustaining capabilities.

What is the Cybersecurity Planning Committee Charter?

The Cybersecurity Planning Committee is directed by a charter that governs the Cybersecurity Planning Committee. All members of the Cybersecurity Planning Committee must sign and date the charter. The charter must be submitted at the time of application as an attachment in ND Grants. Revisions to the charter can be made but must be sent to their assigned FEMA Preparedness Officer.

The Cybersecurity Planning Committee Charter must have:

- A detailed description of the Cybersecurity Planning Committee's composition and an explanation of key governance processes;
- A description of the frequency at which the Cybersecurity Planning Committee will meet;
- An explanation as to how the committee will leverage existing governance bodies;
- A detailed description of how decisions on programmatic priorities funded by TCGP will be made and how those decisions will be documented and shared with its members and other stakeholders, as appropriate; and
- A description of defined roles and responsibilities for financial decision making and meeting administrative requirements.

How should planning committees prioritize individual projects?

Individual projects must help achieve the goal and objectives of the tribe's Cybersecurity Plan. To prioritize projects, the committee should:

- Coordinate activities across preparedness disciplines and within levels of a Tribal Nation;
- Devise a cohesive planning framework;
- Incorporate CISA and FEMA resources as well as those from other entities, as appropriate (e.g., private sector); and
- Determine how available preparedness funding sources can effectively support a whole community approach to emergency preparedness and management and the enhancement of core capabilities.

CYBERSECURITY PLANS

Who is required to submit a Cybersecurity Plan?

Tribal Nations must submit Cybersecurity Plans for review and approval as part of their grant applications in order to receive funding if selected.

Who must approve the Cybersecurity Plan before it is submitted to DHS?

The Cybersecurity Planning Committee and the CIO, CISO or CIO/CISO-equivalent official must approve the Cybersecurity Plan and individual projects before submitting to DHS.

Can I revise my Cybersecurity Plan?

Yes. After initial Cybersecurity Plans are submitted and approved by CISA, Tribal Nations can revise their Cybersecurity Plan as needed. CISA considers the Cybersecurity Plans as living strategic documents. Tribal Nations may also continue to work with CISA regional staff on Cybersecurity Plans and use grant funding once approved for efforts to revise their plan.

Are there specific requirements for the Cybersecurity Plan?

The Cybersecurity Plan should establish high level goals and finite objectives to reduce specific cybersecurity risks across the Tribal Nations. The Cybersecurity Plan should also serve as the overarching framework for the achievement of TCGP goals, with grant-funded projects working to achieve outcomes.

In implementing the Cybersecurity Plan, the Cybersecurity Planning Committee should consider:

- Existing governance and planning documents and identification of any planning gaps that should be addressed by the Cybersecurity Plan;
- Existing assessments and evaluations (e.g., reports, after action reports) conducted by or for the Tribal Nation and any planning gaps that require additional assessments and/or evaluations; and
- Identification of potential TCGP projects to address planning gaps and prioritize mitigation efforts.

The full list of requirements for the Cybersecurity Plan are available in Appendix C in the NOFO.

Is DHS able to provide technical assistance to help with Cybersecurity Plan revision?

CISA Regional Staff will work with tribes individually upon request to help revise their Cybersecurity Plans during the application process. A perfect initial plan is not required, and Tribal Nations should instead focus on submitting a plan with their application. CISA Regional Staff are also available to assist Tribal governments in revising their Cybersecurity Plans post-award.

Can funds be used to enhance existing efforts?

Yes. Grant funds can be used to expand existing efforts if those funds are not used to supplant existing funds and activities involve improvements to cyber systems and meet the required elements.

The projects should achieve a sustainable improvement or solution that will remain even after the expiration of the cybersecurity grant program. The goal of the program as stated in the legislation will be to award grants to address cybersecurity risks and threats to information systems owned or operated by, or on behalf of, Tribal Nations.

Can existing plans be used?

Eligible Tribal Nations are encouraged to incorporate, where applicable, any existing plans to protect against cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of that Tribal Nation. For the required Cybersecurity Plan submission, Tribal Nations can leverage an existing Cybersecurity Plan if it meets the requirements for Cybersecurity Plans outlined in the NOFO.

What will DHS do with the Cybersecurity Plan?

Once approved by the Cybersecurity Planning Committee and the CIO, CISO, or equivalent official, CISA will review each submitted Cybersecurity Plan. Tribal Nations' Cybersecurity Plans will inform the selection of a project in the event two IJs receive the same score during the discretionary review process. Following selections, CISA will approve Cybersecurity Plans and assist Tribal Nations with revision as requested.

Is there a template or guidance for the Cybersecurity Plan?

Yes. CISA offers a downloadable Cybersecurity Plan Template which is also available on Grants.gov with the other TCGP application documents. This template may be used by Tribal Nations or may be referenced as necessary. The template is located on the CISA.gov website.

ADDITIONAL INFORMATION

Where can I go for more information?

For more information, please visit cisa.gov/cybergrants.

What other resources are available to address programmatic, technical and financial questions?

- For additional support and guidance on cybersecurity, Tribal Nations should reach out to their CISA Regional Staff. For contact information for each region, please visit cisa.gov/about/regions or via e-mail at: TCGPinfo@cisa.dhs.gov.
- For additional technical assistance, applicants may contact DHS/FEMA via e-mail at: FEMA-TCGP@fema.dhs.gov.