FY 2023 Tribal Cybersecurity Grant Program (TCGP) Cybersecurity Plan Template User Guide

September 2023

General Information

- This guide is intended to help applicants complete the Fiscal Year (FY) 2023 TCGP Cybersecurity Plan Template and includes key tips and instructions for specific sections of the template in the order in which they appear on the form.

- The template is a Microsoft Word document which is currently in draft format; however, **this draft form should be completed by tribal applicants as part of the TCGP application.**
- Acronyms:
  - **CIO:** Chief Information Officer
  - **CISO:** Chief Information Security Officer
  - **IJ:** Investment Justification
  - **PW:** Project Worksheet
  - **FEMA**: Federal Emergency Management Agency
  - **TCGP:** Tribal Cybersecurity Grant Program

Helpful Hints

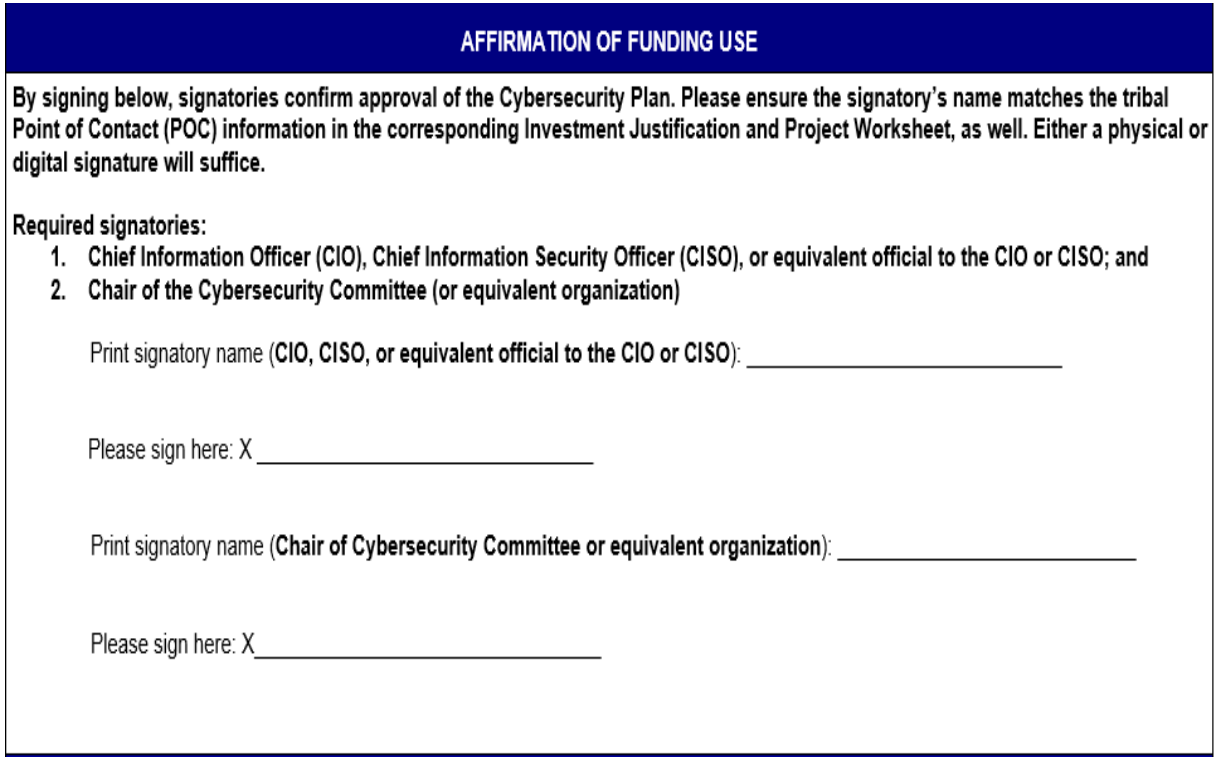
- Complete all required fields prior to submission of your template. Incomplete submissions may delay the review and approval of associated projects and your grant application.
- Editing functionality is limited in the template. Do NOT copy and paste content from Microsoft Word into the template as this may result in issues with spacing and formatting during the drafting process.
- Please reach out to your assigned FEMA Preparedness Officer if you require additional technical assistance with completing this Cybersecurity Plan Template. Or send an email to the TCGP mailbox: FEMA-TCGP@fema.dhs.gov.

FEMA

AFFIRMATION OF FUNDING USE

Affirmation of Funding Use

- The Chief Information Officer (CIO), Chief Information Security Officer (CISO), or equivalent official to the CIO or CISO must match the officials on the Investment Justification (IJ) and Project Worksheet (PW).
- Please print and sign the signatory's name of 1) the CISO, CISO, or equivalent official to the CIO or CISO; and 2) Chair of the Cybersecurity Committee (or equivalent organization).



AFFIRMATION OF FUNDING USE

By signing below, signatories confirm approval of the Cybersecurity Plan. Please ensure the signatory's name matches the tribal Point of Contact (POC) information in the corresponding Investment Justification and Project Worksheet, as well. Either a physical or digital signature will suffice.

Required signatories:

1. **Chief Information Officer (CIO), Chief Information Security Officer (CISO), or equivalent official to the CIO or CISO; and**
2. **Chair of the Cybersecurity Committee (or equivalent organization)**

Print signatory name (**CIO, CISO, or equivalent official to the CIO or CISO**): _____

Please sign here: X _____

Print signatory name (**Chair of Cybersecurity Committee or equivalent organization**): _____

Please sign here: X _____

FEMA

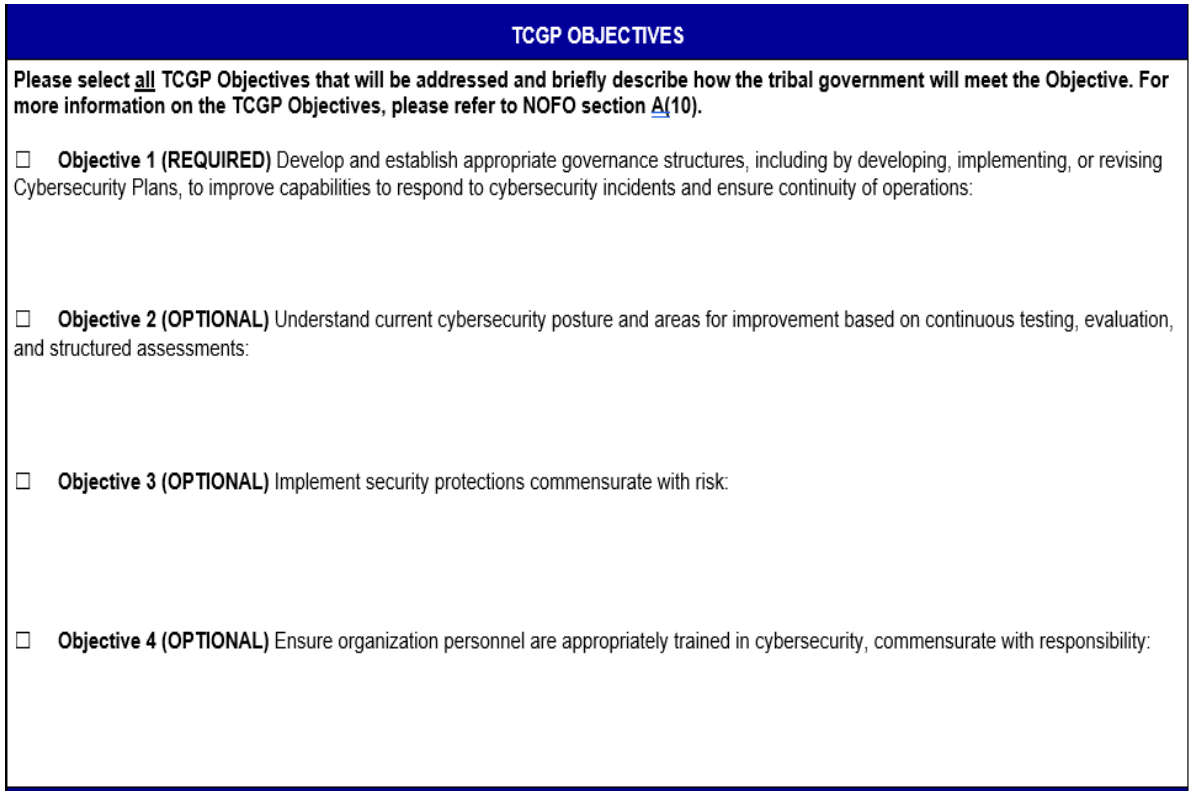
TCGP OBJECTIVES

TCGP Objectives

- The goal of TCGP is to assist tribal governments with managing and reducing systemic cyber risk. Accomplishment of this goal can be achieved by implementing or revising Cybersecurity Plans, priorities, projects and addressing TCGP objectives.

- It is **required** for tribes to submit a project that coincides with Objective 1 for FY 2023. The remaining three objectives are **optional** depending on the tribal government's cybersecurity posture.

- Additional information on the TCGP program objectives can be found in **Appendix A** of the funding opportunity.



TCGP OBJECTIVES

Please select all TCGP Objectives that will be addressed and briefly describe how the tribal government will meet the Objective. For more information on the TCGP Objectives, please refer to NOFO section A(10).

☐ **Objective 1 (REQUIRED)** Develop and establish appropriate governance structures, including by developing, implementing, or revising Cybersecurity Plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations:

☐ **Objective 2 (OPTIONAL)** Understand current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments:

☐ **Objective 3 (OPTIONAL)** Implement security protections commensurate with risk:

☐ **Objective 4 (OPTIONAL)** Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility:

FEMA

13 CYBERSECURITY PLAN ELEMENTS

13 Cybersecurity Plan Elements

Please check one of the below options to indicate the tribal government's assessment of its current capabilities regarding the Cybersecurity Plan element.

☐ Basic
☐ Intermediate
☐ Advanced

What metric(s) will the tribal government use to measure progress toward implementing this planning element?

- Applicants are required to briefly describe how their tribal government will meet the 13 cybersecurity plan elements outlined in the funding opportunity.
- The Cybersecurity Plan must describe how the tribal government plans to address the 13 elements.
  - For tribal governments with existing cybersecurity plans that meet the 13 required elements, references to those plans may be used in place of describing the entire plan in this section.
- Tribal entities are strongly encouraged to expand their Cybersecurity Plans beyond the required elements.
  - An example may include a focus on specific critical infrastructure.

FEMA

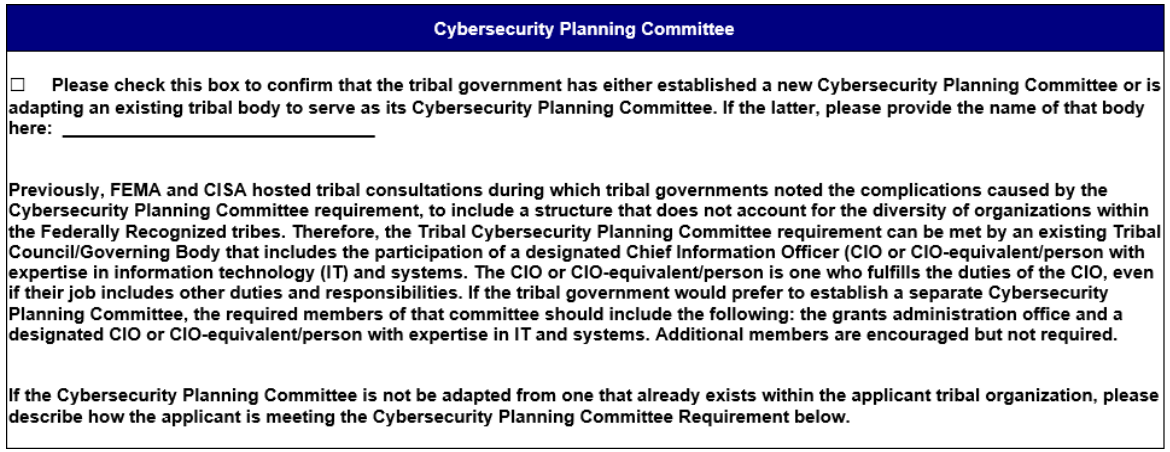
CYBERSECURITY PLANNING COMMITTEE

Cybersecurity Planning Committee

- The Cybersecurity Planning Committee must include:
  - The tribal government applicant;
  - CIO, CISO, or equivalent official to the CIO or CISO; and
  - Grants administrative office.
  - Additional tribal members are encouraged, but not required.

- Eligible entities must submit the list of Cybersecurity Planning Committee members at the time of application as an attachment in ND Grants.

- Additional information on the Cybersecurity Planning Committee can be found in **Appendix B** of the funding opportunity.

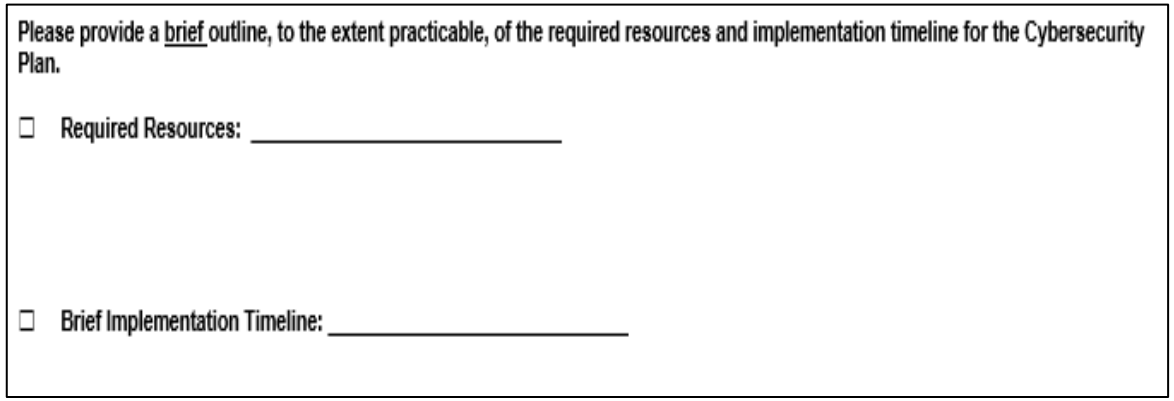


Cybersecurity Planning Committee

☐ Please check this box to confirm that the tribal government has either established a new Cybersecurity Planning Committee or is adapting an existing tribal body to serve as its Cybersecurity Planning Committee. If the latter, please provide the name of that body here: _____

Previously, FEMA and CISA hosted tribal consultations during which tribal governments noted the complications caused by the Cybersecurity Planning Committee requirement, to include a structure that does not account for the diversity of organizations within the Federally Recognized tribes. Therefore, the Tribal Cybersecurity Planning Committee requirement can be met by an existing Tribal Council/Governing Body that includes the participation of a designated Chief Information Officer (CIO or CIO-equivalent/person with expertise in information technology (IT) and systems. The CIO or CIO-equivalent/person is one who fulfills the duties of the CIO, even if their job includes other duties and responsibilities. If the tribal government would prefer to establish a separate Cybersecurity Planning Committee, the required members of that committee should include the following: the grants administration office and a designated CIO or CIO-equivalent/person with expertise in IT and systems. Additional members are encouraged but not required.

If the Cybersecurity Planning Committee is not be adapted from one that already exists within the applicant tribal organization, please describe how the applicant is meeting the Cybersecurity Planning Committee Requirement below.



Please provide a brief outline, to the extent practicable, of the required resources and implementation timeline for the Cybersecurity Plan.

☐ Required Resources: _____

☐ Brief Implementation Timeline: _____

FEMA

TCGP Grant Program Contact Information and Resources

- Lisa Nine, Senior Program Analyst and Team Lead: 202-706-3176, Lisa.Nine@fema.dhs.gov: R10
  - Amanda Carver, Preparedness Officer: 202-368-8197, Amanda.Carver@fema.dhs.gov: R6, R7, R8
  - Amanda Lemminga, Preparedness Officer: 202-924-3436, Amanda.Lemminga@fema.dhs.gov: R2, R3,R4
  - Jennifer Havas Joy, Preparedness Officer: 771-217-7053, Jennifer.Havasjoy@fema.dhs.gov: R1, R5, R9

- TCGP Mailbox: FEMA-TCGP@fema.dhs.gov
- Please reference the Tribal Cybersecurity Grant Program web page on FEMA.gov

Thank you!

FEMA