The Department of Homeland Security (DHS)

Notice of Funding Opportunity (NOFO)

Fiscal Year (FY) 2025 Tribal Cybersecurity Grant Program (TCGP)

Fraud, waste, abuse, mismanagement, and other criminal or noncriminal misconduct related to this program may be reported to the Office of Inspector General (OIG) Hotline. The toll-free numbers to call are 1 (800) 323-8603 and TTY 1 (844) 889-4357.

Contents

1. Basic Information

A. Agency Name	U.S. Department of Homeland Security (DHS), Federal Emergency Management Agency (FEMA)
B. NOFO Title	Fiscal Year (FY) 2025 Tribal Cybersecurity Grant Program (TCGP)
C. Announcement Type	Initial
D. Funding Opportunity Number	DHS-25-GPD-137-00-98

E. Assistance Listing Number	97.156
F. Expected Total Funding	$12,164,971
G. Anticipated Number of Awards	18 awards
H. Expected Award Range	$38,947 – $2,743,512
I. Projected Application Start Date	08/01/2025 4:00 p.m. Eastern Time (ET)
J. Projected Application End Date	08/15/2025 05:00 p.m. ET
K. Anticipated Funding Selection Date	09/04/2025
L. Anticipated Award Date	09/19/2025
M. Projected Period of Performance Start Date	09/01/2025
N. Projected Period of Performance End Date	08/31/2029
O. Executive Summary	Our nation faces unprecedented threats to the homeland from increasingly sophisticated criminal groups and nation-state actors. State, local, Tribal, and territorial (SLTT) entities stand at the forefront of cyber defense. This partnership includes enforcing laws, assisting the federal government in securing borders and cyberspace, and dismantling transnational criminal organizations. Cybersecurity threats, including ransomware intrusions, and widespread software vulnerabilities affecting SLTT systems and critical infrastructure are increasingly exploited by malicious actors, operating both domestically and abroad. To strengthen the essential partnership DHS maintains with its SLTT partners in executing its mission, DHS is committed to supporting SLTT efforts to combat cybersecurity threats and mitigate risks that endanger these vital functions. Considering the risk and potential consequences of cyber incidents, strengthening the cybersecurity practices and resilience of Tribal governments is an important homeland security mission and the primary focus of TCGP. This program enables DHS to make targeted cybersecurity investments in Tribal governments, thus improving the security of critical infrastructure and improving the resilience of the services Tribal governments provide their communities.

P. Agency Contact	**a. *TCGP Program Office Contact*** The FEMA TCGP Program Office can provide general information on all FEMA grant programs and additional guidance surrounding questions on TCGP administration. Applicants and recipients may contact their FEMA Preparedness Officer, the Cyber Section Chief, or the Cyber Branch Chief for more information by email at FEMA-TCGP@fema.dhs.gov. **b. *CISA Grant Program Office Contact*** The Cybersecurity and Infrastructure Security Agency (CISA) Grant Program Office, including programmatic and regional staff, are available to provide general information regarding the TCGP and additional guidance surrounding programmatic requirements and performance metrics. Applicants and recipients can contact their CISA grant program staff and regional staff for more information by email at TCGPinfo@mail.cisa.dhs.gov. **c. *FEMA Grants News*** This channel provides general information on all FEMA grant programs and maintains a comprehensive database containing key personnel contact information at the federal, state, and local levels. FEMA Grants News Team is reachable at fema-grants-news@fema.dhs.gov OR (800) 368-6498, Monday through Friday, 9:00 AM – 5:00 PM ET. **d. *Grant Programs Directorate (GPD) Award Administration Division*** GPD's Award Administration Division (AAD) provides support regarding financial matters and budgetary technical assistance. AAD can be contacted at ASK-GMD@fema.dhs.gov. **e. *Civil Rights*** Consistent with Executive Order 14173, *Ending Illegal Discrimination & Restoring Merit-Based Opportunity*, the FEMA Office of Civil Rights is responsible for ensuring compliance with and enforcement of federal civil rights obligations in connection with programs and services conducted by FEMA. They are reachable at FEMA-CivilRightsOffice@fema.dhs.gov **f. *Environmental Planning and Historic Preservation*** The FEMA Office of Environmental Planning and Historic Preservation (OEHP) provides guidance and information about the EHP review process to FEMA programs and recipients and subrecipients. Send any inquiries regarding compliance for FEMA

	grant projects under this NOFO to FEMA-OEHP-NOFOQuestions@fema.dhs.gov. **g. *FEMA GO*** For technical assistance with the FEMA GO system, please contact the FEMA GO Helpdesk at femago@fema.dhs.gov or (877) 585-3242, Monday through Friday, 9:00 AM – 6:00 PM ET.

2. Eligibility

A. Eligible Entities/Entity Types	Only the following entities or entity types are eligible to apply. **a. *Applicants*** The only eligible Tribal applicants are those listed in Section 3 of this Notice of Funding Opportunity, "FY 2025 TCGP Target Allocations." FY 2025 TCGP applications are limited to only those meritorious applicant projects and investments as identified by FEMA in individual notifications to the eligible Tribal governments. "Tribal government" is defined at Section 2220A(a)(7) of the Homeland Security Act of 2002 (codified as amended at 6 U.S.C. § 665g(a)(7)) 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 published list of Federally Recognized Tribes. **b. *Sub-applicants and subawards*** Sub-applicants and subawards are allowed for TCGP. Subapplicants should not have foreign nationals or noncitizens included. If a sub-applicant has foreign nationals, they must be properly vetted and must adhere to all government statues, polices, and procedures including "staff American, stay in America" and security requirements. Eligible subrecipients to not include nonprofit or for-profit organizations.
B. Project Type Eligibility	**a. *Unallowable Project Types*** Unallowable project types are described in Section 3.G, "Program-Specific Unallowable Costs" in this NOFO. **b. *Allowable Project Types*** Please see the Appendix E, "Planning, Organization, Equipment, Training, and/or Exercises (POETE) Solution Areas for Investment" for more information on allowable costs related to the POETE Solution Areas.

	Allowable TCGP costs, pre-award costs, M&A costs, and indirect costs are described in Section 3.H - 3.J.
C. Requirements for Personnel, Partners, and Other Parties	Not applicable.
D. Maximum Number of Applications	The maximum number of applications that can be submitted is: 1. A maximum of one application per eligible tribal government.
E. Additional Restrictions	Applicants/subapplicants or recipients/subrecipients are required to certify their compliance with federal statutes, DHS directives, policies, and procedures.
F. References for Eligibility Factors within the NOFO	Please see the following references provided below: 1. "Responsiveness Review Criteria" subsection 2. "Financial Integrity Criteria" subsection 3. "Supplemental Financial Integrity Criteria and Review" subsection 4. FEMA may/will request financial information such as Employer Identification Number (EIN) and bank information as part of the potential award selection. This will apply to everyone prospered, including subrecipients
G. Cost Sharing Requirement	Applicants selected for this award must agree to an acceptable cost share agreement. Otherwise, they will not be funded. Project-based Cost Share: Section 2220A of the Homeland Security Act of 2002 requires recipients to meet a non-federal matching requirement for an "activity" carried out under an TCGP grant award. DHS interprets the term "activity" to be an approved "project" under a TCGP grant award and administers the nonfederal matching requirement in accordance with 2 C.F.R. § 200.306. Eligible applicants must agree to make available non-federal funds to carry out a TCGP award in an amount not less than 40% of the total project costs (federal award amount plus cost share amount, rounded to the nearest whole dollar). The cost share for the multi-entity projects is 30% for FY 2025. **Cost Share Waiver** The Secretary of Homeland Security (or designee) may waive or modify the non-federal share for an individual entity if the entity demonstrates economic hardship. The Homeland Security Act of 2002, as amended, requires TCGP recipients in FY 2025 to provide a non-federal cost share of 40% if they are applying as a single entity (6 U.S.C. § 665g(m)(1)). However, DHS is not able to provide additional funds even if it does grant a cost share waiver. The federal funding will remain at the same amount as indicated by the statutory formula.

All Cost Share Waiver requests must be submitted post-award by the eligible entity by emailing the request and supporting documentation to FEMA-TCGP@fema.dhs.gov.

Economic Hardship Factors

The Secretary of Homeland Security (or designee) may consider the following factors when determining economic hardship or the Secretary may waive or modify the following requirements for 1 or more Tribal governments if the Secretary determines that a waiver is in the public interest:

a. Changes in rates of unemployment in the jurisdiction from previous years;
b. Changes in the percentage of individuals who are eligible to receive benefits under the supplemental nutrition assistance program established under the Food and Nutrition Act of 2008 (7 U.S.C. § 2011 et seq.) from previous years; and
c. Any other factors the Secretary considers appropriate.

To be considered for a cost share waiver, eligible entities must meet at least one of the three factors described above, but do not necessarily need to meet all of them. Requests for waivers will be considered on a case-by-case basis and evaluated holistically. The applicant is required to submit documentation supporting their request for an Economic Hardship Cost Share Waiver at the award level post-award by attaching the supporting document to the grant application.

Cost Share Waiver Request Requirements

To request a waiver, an eligible entity must submit a written narrative, including the following three categories to demonstrate economic hardship by emailing the request and supporting documentation to FEMA-TCGP@fema.dhs.gov:

a. History: A description of the entity's background/history of economic hardship.
b. Austerity: Describe any measures the entity has taken to address economic hardship.
c. Operational Impact: Describe how the lack of a waiver will impact the entity's ability to develop, implement, or revise a Cybersecurity Plan or address imminent cybersecurity threats.

A detailed justification explaining why the Tribal government (or specific project(s) if requesting only a partial waiver) is unable to fulfill the cost share requirement. The applicant must identify specific economic hardship(s) and address the factors listed above.

	Approval Process Once a decision on a waiver request is made, the Tribal government will be notified in writing. If approved, the award package will indicate that the cost share has been waived in full or in part. The cost share waiver will be included in the post-award requirements for submission of the Project Worksheet and detailed Budget Worksheet and Budget Narrative found in Appendix B. If the waiver request is approved after the award has been issued, FEMA will amend the award package to indicate that the cost share has been waived in full or in part and whether the recipient must submit a revised budget and/or scope (as applicable) for the identified project(s). Questions regarding the cost share waiver process may be directed to your FEMA Preparedness Officer by emailing FEMA-TCGP@fema.dhs.gov.
H. Cost Share Description, Type and Restrictions	DHS administers cost-matching requirements in accordance with 2 C.F.R. § 200.306. To meet matching requirements, the recipient contributions must be verifiable, reasonable, allocable, and necessary, and otherwise allowable under the grant program, and in compliance with all applicable federal requirements and regulations. The non-federal cost share requirement cannot be matched with other federal funds, unless specifically authorized by the legislation governing that other source of federal funding. The cost share applies to each project funded by the grant award rather than just to the cumulative total of all projects. Recipients must ensure that each project's cost share is met. A Project Worksheet (PW) must include cost share for each project as well as Management and Administration (M&A). M&A must be included as a separate row in the PW. Also, the PW must include a description of the source of the cost share. Note for post-award documentation of cost share, if funds or services are to be provided by a third-party for in-kind match, a dated letter of commitment is required to document the donation. The recipient contribution can be cash (hard match) or third-party in-kind (soft match). Types of Cost Share/Match 1. Hard Match (Cash) Cash or hard matching includes cash spent for project-related costs. The allowable cash match must include costs that are necessary,

	reasonable, and allowable under the TCGP. Tribal general fund monies are an example of hard match. 2. Soft Match (In-kind) Soft match refers to contributions of the reasonable value of property or services in lieu of cash which benefit a federally assisted project or program. This type of match may only be used if not restricted or prohibited by program statute, regulation, or guidance and must be supported with source documentation. Only property or services that comply with program guidance and/or program regulations, are allowable. In other words, a recipient cannot use a source for the soft match that is completely unrelated to the TCGP's goals, objectives, and allowable costs identified in the NOFO, etc. The same contribution cannot be used if it is already used as match for another grant program or paid from other grant funds. Below are some examples of allowable soft match: a. Example 1: A hotel offers a room or space to conduct a cybersecurity training event or tabletop exercise. The hotel manager should provide the Tribal government with written documentation of the room rental (dollar value), date/time of the donation, signed by the hotel manager. This should align with the date/time of the training or exercise event. And, per 2 C.F.R. 200.306, "The value of donated space must not exceed the fair rental value of comparable space as established by an independent appraisal of comparable space and facilities in a privately-owned building in the same locality." b. Example 2: Contributions of salary, travel, equipment, supplies, and other budget areas that are from third-party sources (in compliance with 2 C.F.R. 200.306) and include voluntary contributions such as emergency personnel, lawyers, etc., who donate their time to a federal grant program. The normal per hour rate for these professionals (acting in their professional capacity) can be used to meet the matching requirement. The value of the services provided is taken into consideration when determining the value of the contribution and not who is providing the service. For example, if a lawyer is volunteering his/her services to assist the Cybersecurity Planning Committee with preparing and filing legal paperwork for their Charter, the lawyer's normal hourly rate is allowable. However, if the lawyer is volunteering his/her time and services to conduct cybersecurity needs assessments as part of the Tribal government's cybersecurity plan implementation, the lawyer's hourly rate would not be applicable. Instead, the hourly rate for an information technology specialist would be more reasonable and applicable.

I. Cost Sharing Calculation Example	Calculating Cost Share for the Application on the Project Worksheet Formula: Federal Award Amount / Federal Share Percentage = Total Project Cost Cost Share Percentage = Cost Share Amount (rounded up to the nearest whole dollar) Example: If the federal award is $1,000,000 with a 60% federal share percentage and a 40% cost share percentage, the cost share amount is calculated below: • $1,000,000 (Federal Award Amount) / .60 = $1,666,666.67 (Total Project Cost) • $1,666,666.67 x .40 = $666,667 (Cost Share Amount rounded to the next whole dollar) Calculating Cost Share for Projects on the Project Worksheet Cost share must be provided on a project basis. To calculate cost share for a project, please see the following formula and example: Formula: Total Project Cost x Cost Share Percentage of the Project = Cost Share Amount; Total Project Cost x Federal Percentage Share of the Project = Federal Amount for the Project Example: If the total project cost is $125,000, the cost share percentage of the project is 40% and the federal percentage share of the project is 60%, the cost share amount for the project and federal amount for the project is calculated below: • $125,000 x .40 = $50,000 (Cost Share Amount for Project) • $125,000 x .60 = $75,000 (Federal Share Amount for Project)
J. Required information for verifying Cost Share	Applicants are not required to submit documents to verify cost share (or match) in the pre-award phase. However, applicants will be required to include the source of the cost share on the Project Worksheet as part of their post-award documentation submission. Cost Share Documentation for soft match: The source documentation for the cost share should be: 1. Valued at the time of the donation—value must not exceed the fair market value of the equipment of the same age and condition at the time of donation. 2. Signed and dated by the donating company, person, etc. 3. For third-party in-kind contributions, the fair market value of goods and services must be documented and, to the extent feasible,

	supported by the same methods used internally by the non-federal entity.

3. Program Description

A. Background, Program Purpose, and Program History

Our nation faces unprecedented threats to the homeland from increasingly sophisticated criminal groups and nation-state actors. SLTT entities stand at the forefront of cyber defense. This partnership includes enforcing laws, assisting the federal government in securing borders and cyberspace, and dismantling transnational criminal organizations. Cybersecurity threats, including ransomware intrusions, and widespread software vulnerabilities affecting SLTT systems and critical infrastructure are increasingly exploited by malicious actors, operating both domestically and abroad. To strengthen the essential partnership DHS maintains with its SLTT partners in executing its mission, DHS is committed to supporting SLTT efforts to combat cybersecurity threats and mitigate risks that endanger these vital functions.

Considering the risk and potential consequences of cyber incidents, strengthening the cybersecurity practices and resilience of Tribal governments is an important homeland security mission and the primary focus of TCGP. Through funding from the Infrastructure Investment and Jobs Act referred to as the Bipartisan Infrastructure Law (BIL) throughout this document, the TCGP enables DHS to make targeted cybersecurity investments in Tribal governments, thus improving the security of critical infrastructure and improving the resilience of the services Tribal governments provide their communities.

FY 2025 TCGP Allocations

The BIL appropriated $300 million in FY 2024 and $100 million in FY 2025 for the state, territorial, local, and tribal cybersecurity grant programs with 3% of the total appropriations being available under the TCGP to eligible recipients. The funding appropriated for the TCGP for FY 2024 and FY 2025 is $9,142,996 for FY 2024 and $3,021,975 for FY 2025. FEMA and CISA combined the funding from both fiscal years into this single TCGP NOFO, for a total of $12,164,971.

For the Fiscal Year 2022/2023 TCGP award cycle, CISA and FEMA created a discretionary allocation structure based on Tribal populations that elicited extensive interest from Tribal governments (e.g., 73 Tribal governments submitted applications for funding exceeding $100 million, far exceeding the available roughly $18 million). The statutory authorization for the TCGP expires on September 30, 2025, after which no new awards can be made. Insufficient time now remains to solicit and receive competitive applications, conduct review panels to evaluate, score and rank applications, and make awards, prior to the September 30, 2025, deadline. Therefore, CISA and FEMA will allocate the remaining $12,164,971 of Fiscal Year 2024/2025 TCGP funding to make additional awards, to fund meritorious Tribal applicant projects which did not receive funding during the Fiscal Year 2022/2023 award cycle. This decision is consistent with and reflects extensive feedback from tribal governments after nation-to-nation consultations (August 2022, November 2023, and September 2024).

Eligible applicants will be notified by FEMA of the specific investments and allocations per investment no later than Monday, August 4, 2025. Final allocation amounts will be

determined and applicants will be notified after the Application Deadline date of August 15, 2025. Target allocations are included below:

FY 2025 TCGP Target Allocations

Tribal Government	Target Allocation
Blackfeet Tribe Total	$1,927,400
Chippewa Cree Total	$2,743,512
Confederated Tribes of the Colville Reservation Total	$643,903
Inupiat Community of the Arctic Slope Total	$573,184
Kickapoo Traditional Tribe of Texas Total	$45,000
Little Traverse Bay Bands of Odawa Indians Total	$70,000
Metlakatla Indian Community Total	$1,215,680
Mohegan Tribe of Indians of Connecticut Total	$265,000
Native Village of Kluti-Kaah Total	$62,973
Nottawaseppi Huron Band of the Potawatomi Total	$1,030,270
Paskenta Band of Nomlaki Indians Total	$247,235
Prairie Band Potawatomi Nation Total	$1,034,938
Quapaw Tribe of Oklahoma Total	$370,678
Saint Regis Mohawk Tribe Total	$20,130
San Carlos Apache Tribal Council Total	$570,815
Seminole Tribe of Florida Total	$1,054,253
Southern Ute Indian Tribe Total	$120,000
Swinomish Indian Tribal Community Total	$170,000
Total	**$12,164,971**

Additional information related to the formula allocation methodology is detailed in Section 7.B., "Application Review Information" of this funding notice.

B. Goal and Objectives and Priorities

a. *Goal*

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.

b. *Objectives*

Listed below are the objectives for the Tribal Cybersecurity Grant Program:

- **Objective 1:** Develop and establish appropriate governance structures, including by implementing or revising Cybersecurity Plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.
- **Objective 2:** Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.

- **Objective 3:** Implement security protections commensurate with risk.
- **Objective 4:** Ensure Tribal organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

FY 2025 Tribal applicants are limited to applying for the investment/objective number and federal amount included in Section 3. Applicants should refer to the TCGP CISA website for more information on TCGP program goals, objectives, sub-objectives, and desired outcomes required in their FY 2025 TCGP application.

c. *Priorities*

Cybersecurity Plan, Committee Membership List, and Charter

The Homeland Security Act of 2002, as amended by the BIL, requires TCGP grant recipients to develop a Cybersecurity Plan, establish a Cybersecurity Planning Committee to support development of the Cybersecurity Plan, and identify projects to implement using TCGP funding. To support these efforts, recipients must prioritize the following activities using FY 2025 TCGP funds, all of which are statutorily required as a condition of receiving a grant:

- Establish a Cybersecurity Planning Committee;[1] and
- Implement or revise a Cybersecurity Plan.[2]

Cybersecurity Activities

The tribal government must consult with its CIO, CISO, or equivalent official to the CIO or CISO (who fulfills the duties of the CIO or CISO, even if their job includes other duties and responsibilities), in the plans for allocating TCGP funds. To support the FY 2025 TCGP requirements, Cybersecurity Plans must include the following activities:

i. An assessment of the capabilities of the tribal government relating to the 13 required cybersecurity plan elements;[3] and

ii. Adopting key cybersecurity best practices and consulting **Cybersecurity Performance Goals (CPGs)**.[4]
   a. The CPGs are a prioritized subset of information technology and operational technology cybersecurity practices aimed at meaningfully reducing risks to critical infrastructure operations.
   b. These goals are applicable across all critical infrastructure sectors and are informed by the most common and impactful threats and adversary tactics, techniques, and procedures (TTPs) observed by CISA and its government and industry partners,

[1] 6 U.S.C. § 665g(g). An existing Tribal Council/Governing Body that includes the participation of 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) and systems. The CIO, CISO, or equivalent official to the CIO or CISO 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 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. 6 U.S.C. § 665g(h).

[2] 6 U.S.C. §§ 665g(e) and 665g(h).

[3] 6 U.S.C. §§ 665g(e)(2)(B)(i)-(xiii).

[4] 6 U.S.C. § 665g(e)(2)(B)(v).

making them a common set of protections that all critical infrastructure entities – from large to small – should implement.

c. The CPGs do not reflect an all-encompassing cybersecurity program – rather, they are a minimum set of practices that organizations should implement towards ensuring a strong cybersecurity posture.
d. The Cross-Sector Cybersecurity Performance Goals are regularly updated, with a targeted revision cycle of at least every 6 to 12 months.

Key Cybersecurity Best Practices for Individual Projects

To keep pace with today's dynamic and increasingly sophisticated cyber threat environment, Tribal governments must take decisive steps to modernize their approach to cybersecurity. As tribes increase their cybersecurity maturity, CISA recommends they move toward implementing more advanced best practices, such as endpoint detection and response capabilities, as well as conducting regular penetration testing. To assist in the revision of tribal cyber planning efforts, the following Cybersecurity Best Practices are provided. As appropriate, the strategic elements listed in the table below should be included in FY 2025 individual projects:

Cybersecurity Best Practices for Individual Projects
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 sharing between CISA and Tribal governments in cyber relevant time frames to drive down cyber risk
Migration to the .gov internet domain

Cybersecurity Investments and Projects

Given the Cybersecurity Plan is a strategic document, it should not identify specific vulnerabilities but instead capture the broad level of capability across the tribal government. The Cybersecurity Plan must also show how the implementation of the individual projects and activities over time will help achieve the goals and objectives of the plan. A summary of projects using FY 2025 TCGP funds associated with each required and discretionary element provides a helpful snapshot of tribal capabilities and capacity that will be achieved as a result of this funding. Details for each project using TCGP funds must be included in the IJs.

Each IJ must provide a baseline understanding of the existing cybersecurity gaps, risks, and threats that the applicant entity faces, which have influenced the development of the IJ. The IJ must include a summary of the current capabilities within the applicant tribal government to address these threats and risks. The IJ should also include a description of how the proposed project addresses gaps and/or sustainment in the Cybersecurity Plan and how the project aligns to the cybersecurity elements in this funding notice. Finally, the IJ should include implementation planning data to assist in project management.

The Project Worksheet (PW), Budget Worksheet and Budget Narrative will be used to identify the budget details portion of the application. As part of the post-award process found in Appendix B: Post-Award Program-specific Required Documents, Forms and Information, eligible applicants must submit only one PW as part of the overall application and must include information for each IJ submitted as part of the application for funding. More information on the IJ Template, PW and instructions can be found in Section 4.D., "Program Specific Required Documents and Information" in this funding notice.

Imminent Cybersecurity Threat

TCGP is primarily a security preparedness program focused on reducing cyber risks by helping Tribal governments address cybersecurity vulnerabilities and build cybersecurity capabilities. Over time, the program activities and investments reduce the potential impact of cybersecurity threats and incidents. Section 2220A(d)(4) of the Homeland Security Act of 2002 (codified as amended at 6 U.S.C. § 665g(d)(4)) provides that:

> An eligible entity that receives a grant under this section and a local government that receives funds from a grant under this section, as appropriate, shall use the grant to assist with activities that address imminent cybersecurity threats, as confirmed by the Secretary, acting through the [CISA] Director, to the information systems owned or operated by, or on behalf of, the eligible entity or a local government within the jurisdiction of the eligible entity.

The following provides an overview of the imminent cybersecurity threat process for the FY 2025 grant cycle. Specific details on CISA's criteria and process for confirming an imminent cybersecurity threat are not included here. The following also does not supersede or replace existing threat notification procedures or existing methods to collaborate on operational cybersecurity matters.

Process Overview

- Any eligible entity seeking to use TCGP funds to address an imminent cybersecurity threat, as confirmed by the Secretary, acting through the CISA Director, must have a Cybersecurity Plan approved by CISA.
- DHS, through CISA, will determine whether an incident constitutes an imminent cybersecurity threat.
- Upon confirmation, DHS will notify the tribal recipient who will, in turn, notify the Cybersecurity Planning Committee and CIO, CISO, or equivalent official to the CIO or CISO.
- DHS will notify impacted Tribal governments, as appropriate, of permissible imminent cybersecurity threat fund usage.
- FEMA will issue an Information Bulletin (IB) detailing the impacted governments and procedures for reprograming TCGP funds to support the specific imminent cybersecurity threat. The scope of the IB will be dependent on the nature of the imminent cybersecurity threat.

C. Program Rationale

FY 2025 TCGP is authorized under the Homeland Security Act of 2002, Pub. L. No. 107-296, § 2220A (codified as amended at 6 U.S.C. § 665g).

D. Federal Assistance Type
Grant

E. Performance Measures and Targets

DHS will communicate with all TCGP recipients on the information collection process related to performance measures data. DHS will measure the recipient's performance of the grant by comparing the number of activities and projects needed and requested in its IJs with the number of activities and projects acquired and delivered by the end of the period of performance (POP) using the following programmatic metrics:

	Performance Measures
1	Percentage of tribes with CISA approved tribal Cybersecurity Plans (100% target range – statutorily required)
2	Percentage of tribes with Tribal Cybersecurity Planning Committees that meet the Homeland Security Act of 2002 and TCGP funding notice requirements (100% target range– statutorily required)
3	Percentage of tribes conducting annual table-top and full-scope exercises to test Cybersecurity Plans (40% target range)
4	Percent of the tribes' TCGP budget allocated to exercises (10% target range)
5	Average dollar amount expended on exercise planning for tribes (10% target range)
6	Percentage of tribes conducting an annual cyber risk assessment to identify cyber risk management gaps and areas for improvement (70% target range)
7	Percentage of tribes performing phishing training (50% target range)
8	Percentage of tribes conducting awareness campaigns (90% target range)
9	Percent of tribes providing role-based cybersecurity awareness training to employees (60% target range)
10	Percentage of tribes with capabilities to analyze network traffic and activities related to potential threats (60% target range)
11	Percentage of tribes implementing multi-factor authentication (MFA) for all remote access and privileged accounts (70% target range)
12	Percentage of tribes with programs to anticipate and discontinue use of end-of-life software and hardware (60% target range)
13	Percentage of tribes prohibiting the use of known/fixed/default passwords and credentials (75% target range)
14	Percentage of tribes operating under the ".gov" internet domain (50% target range)
15	Number of cybersecurity gaps or issues addressed annually by tribes (50% target range)
16	Percentage of tribes-created performance metrics that were met (50% target range)
17	Percentage of tribes participating in CISA services (50% target range)
18	Percentage of tribes that have implemented data encryption projects (50% target range)
19	Percentage of tribes that have implemented enhanced logging projects (60% target range)

20	Percentage of tribes that have implemented system reconstitution projects (60% target range)

F. General Funding Requirements

Costs charged to federal awards (including federal and non-federal cost share funds) must comply with applicable statutes, rules and regulations, policies, this NOFO, and the terms and conditions of the federal award. This includes, among other requirements, that costs must be incurred, and products and services must be delivered within the budget period. 2 C.F.R. § 200.403(h).

Recipients may not use federal funds or any cost share funds for the following activities:

1. Matching or cost sharing requirements for other federal grants and cooperative agreements (see 2 C.F.R. § 200.306).
2. Lobbying or other prohibited activities under 18 U.S.C. § 1913 or 2 C.F.R. § 200.450.
3. Prosecuting claims against the federal government or any other government entity (see 2 C.F.R. § 200.435).

G. Indirect Costs (Facilities and Administrative Costs)

Indirect costs are allowed for recipients.

Indirect costs (IDC) are costs incurred for a common or joint purpose benefitting more than one cost objective and not readily assignable to specific cost objectives without disproportionate effort. Applicants with a current negotiated IDC rate agreement who desire to charge indirect costs to a federal award must provide a copy of their IDC rate agreement with their applications. Not all applicants are required to have a current negotiated IDC rate agreement. Applicants that are not required to have a negotiated IDC rate agreement, but are required to develop an IDC rate proposal, must provide a copy of their proposal with their applications. Applicants without a current negotiated IDC rate agreement (including a provisional rate) and wish to charge the de minimis rate must reach out to FEMA for further instructions. Applicants who wish to use a cost allocation plan in lieu of an IDC rate proposal must reach out to FEMA for further instructions. As it relates to the IDC for subrecipients, a recipient must follow the requirements of 2 C.F.R. §§ 200.332 and 200.414 in approving the IDC rate for subawards.

Indirect Cost Agreement or Proposal

Applicants should submit their unexpired, Negotiated Indirect Cost Rate Agreement as an attachment in FEMA GO, if the budget includes indirect costs. Contact the relevant FEMA staff identified in Section 1.P of this notice, "DHS Awarding Agency Contact Information" for further instructions.

Establishing Indirect Cost Rates

The processes for establishing the indirect cost rate vary based on the type of entity and the amount of funding they receive:

1. If the entity is a non-governmental entity, and is a subrecipient, indirect cost rate procedures are outlined in 2 C.F.R. § 200.332(b)(4). These types of entities may either use the de minimis rate or negotiate a rate with the pass-through entity.
2. If the subrecipient is a governmental department or agency, indirect cost rate procedures are established in 2 C.F.R. Part 200, Appendix VII. Per Paragraph D.1.a. of Appendix

VII, all departments or agencies of the governmental unit desiring to claim indirect costs under Federal awards must prepare an indirect cost rate proposal and related documentation to support those costs.

3. If the governmental department or agency receives more than $35 million in grant funding in a fiscal year, the proposal must be approved by the cognizant agency. 2 C.F.R. Part 200, Appendix VII, Paragraph D.1.b.
4. If a governmental department or agency receives $35 million or less in grant funding in a fiscal year, they must develop an indirect cost rate proposal, but that indirect cost rate proposal does not need to be approved by the cognizant agency. 2 C.F.R. Part 200, Appendix VII, Paragraph D.1.c.
5. If a state, local governmental, or tribal entity wants to use the de minimis rate (instead of developing an indirect cost rate proposal), they can request a case-by-case exception from FEMA (per 2 C.F.R. § 200.102(b)).

H. Management and Administration (M&A) Costs

M&A costs are allowed.

A maximum of up to 5% of TCGP funds awarded may be used by the tribal government solely for M&A purposes associated with the TCGP award. Indirect costs and M&A costs are not the same and, therefore, should not be combined on the Project Worksheet application document. For TCGP, allowable M&A are direct costs only. The M&A percentage, amount and purpose should be entered on the Project Worksheet. To request M&A costs, recipients will need to reduce their investment funding amount(s) on the PW and IJ to account for the M&A funding amounts. If an applicant wants to claim indirect costs for their TCGP application, please refer to Section G above and include indirect costs as a separate line item on the Project Worksheet.

M&A costs are for activities directly related to the management and administration of the award, such as financial management, reporting, and program and financial monitoring. Some examples of M&A costs include grants management training for M&A staff, membership fees for M&A staff, equipment and supplies for M&A staff to administer the grant award, travel costs for M&A staff to attend conferences or training related to the grant program, travel costs for the M&A staff to conduct project oversight and monitoring, contractual services to support the M&A staff with M&A activities, and auditing costs related to the grant award to the extent required or permitted by statute or 2 C.F.R. Part 200. All membership costs utilizing TCGP funding must be approved in advance by FEMA.

Characteristics of M&A expenses can include the following:

i. Direct costs that are incurred to administer a particular federal award;
ii. Identifiable and unique to each federal award;
iii. Charged based on the activity performed for that particular federal award; and
iv. Not duplicative of the same costs that are included in the approved Indirect Cost Rate Agreement, if applicable.

I. Program-Specific Unallowable Costs

For FY 2025 TCGP, grant funds may not be used for the following:

a. Spyware;

b. Construction;
c. Renovation;
d. To pay a ransom;
e. For recreational or social purposes;
f. To pay for cybersecurity insurance premiums;
g. Costs associated with the Tribal Information Sharing and Analysis Center (Tribal-ISAC), and the Center for Internet Security (e.g. Election Infrastructure Information Sharing and Analysis Center (EI-ISAC)), including but not limited to membership fees and services;
h. To acquire land or to construct, remodel, or perform alterations of buildings or other physical facilities. This prohibition does not include minor building modifications. Unallowed "alterations" include permanent modifications that substantially affect the building's structure, layout, or systems, affect critical aspects of a building's safety (such as structural integrity, fire safety systems), or other modifications that materially increase the value or useful life of the building.
    - Examples of the types of alterations that are unallowable with TCGP funding, or the non-federal cost share, are listed below:
        - Updating an electrical system to a building which involves work to enhance or modernize the electrical infrastructure, such as replacing electrical panels, upgrading old or unsafe wiring, and replacing circuit breakers. This type of work is likely a modification that substantially affects the building's systems and thus would comprise an alteration.
        - Installing new walls or reconfiguring existing ones.
        - Affixing equipment in such a way that it becomes a permanent part of a building (as this would result in the equipment no longer being personal property).
i. For any purpose that does not address cybersecurity risks or cybersecurity threats on information systems owned or operated by, or on behalf of, the eligible entity that receives the grant or a local government within the jurisdiction of the eligible entity;
j. To supplant state or local funds; however, this shall not be construed to prohibit the use of funds from a grant under this NOFO for otherwise permissible uses on the basis that the SLTT has previously used SLTT funds to support the same or similar uses; and
k. For any recipient or subrecipient cost-sharing contribution.

J. Pre-Award Costs
No pre-award costs are allowable for FY 2025 TCGP.

K. Beneficiary Eligibility
This NOFO and any subsequent federal awards create no rights or causes of action for any beneficiary.

L. Participant Eligibility
This NOFO and any subsequent federal awards create no rights or causes of action for any participant.

M. Authorizing Authority
Homeland Security Act of 2002, Pub. L. No. 107-296, § 2220A codified as amended at 6 U.S.C. § 665g.

N. Appropriation Authority
Infrastructure Investment and Jobs Act, Pub. L. No. 117-58, Division J, Title V

O. Budget Period
There will be only a single budget period with the same start and end dates as the period of performance.

P. Prohibition on Covered Equipment or Services
Recipients, sub-recipients, and their contractors or subcontractors must comply with the prohibitions set forth in Section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019, which restrict the purchase of covered telecommunications and surveillance equipment and services. Please see 2 C.F.R. §§ 200.216, 200.327, 200.471, and Appendix II to 2 C.F.R. Part 200, and FEMA Policy #405-143-1 - Prohibitions on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services for more information.

4. Application Contents and Format

A. Pre-Application, Letter of Intent, and Whitepapers
Not applicable.

B. Application Content and Format
Not applicable.

All application forms are available on Grants.gov or FEMA's TCGP website.

C. Application Components
The following forms or information are required to be submitted via FEMA GO. The Standard Forms (SF) are also available at Forms | Grants.gov.

- SF-424, Application for Federal Assistance
- Grants.gov Lobbying Form, Certification Regarding Lobbying
- SF-LLL, Disclosure of Lobbying Activities

D. Program-Specific Required Documents and Information
There are no program-specific required documents and information at time of application. Program-specific required documents, forms and information will be required from recipients post award. More information can be found in Appendix B. "Program-specific Required Documents, Forms and Information".

E. Post-Application Requirements for Successful Applicants
Not applicable.

5. Submission Requirements and Deadlines

A. Address to Request Application Package

Applications are processed through the FEMA GO system. To access the system, go to https://go.fema.gov/.

Steps Required to Apply For An Award Under This Program and Submit an Application:

To apply for an award under this program, all applicants must:

a. Apply for, update, or verify their Unique Entity Identifier (UEI) number and EIN from the Internal Revenue Service;
b. In the application, provide an UEI number;
c. Have an account with login.gov;
d. Register for, update, or verify their SAM account and ensure the account is active before submitting the application;
e. Register in FEMA GO, add the organization to the system, and establish the Authorized Organizational Representative (AOR). The organization's electronic business point of contact (eBiz POC) from the SAM registration may need to be involved in this step. For step-by-step instructions, see https://www.fema.gov/media-library/assets/documents/181607;
f. Submit the complete application in FEMA GO using the TCGP FEMA GO Application Process (copies can be obtained by emailing FEMA-TCGP@fema.dhs.gov);
g. Continue to maintain an active SAM registration with current information at all times during which it has an active federal award or an application or plan under consideration by a federal awarding agency. As part of this, applicants must also provide information on an applicant's immediate and highest-level owner and subsidiaries, as well as on all predecessors that have been awarded federal contracts or federal financial assistance within the last three years, if applicable.

Per 2 C.F.R. § 25.110(a)(2)(iv), if an applicant is experiencing exigent circumstances that prevents it from obtaining an UEI number and completing SAM registration prior to receiving a federal award, the applicant must notify FEMA as soon as possible. Contact fema-grants-news@fema.dhs.gov and provide the details of the exigent circumstances.

How to Register to Apply:

General Instructions:

Registering and applying for an award under this program is a multi-step process and requires time to complete. Below are instructions for registering to apply for FEMA funds. Read the instructions carefully and prepare the requested information before beginning the registration process. Gathering the required information before starting the process will alleviate last-minute searches for required information.

The registration process can take up to four weeks to complete. To ensure an application meets the deadline, applicants are advised to start the required steps well in advance of their submission.

Organizations must have a Unique Entity Identifier (UEI) number, Employer Identification Number (EIN), and an active System for Award Management (SAM) registration.

Obtain a UEI Number:

All entities applying for funding, including renewal funding, must have a UEI number. Applicants must enter the UEI number in the applicable data entry field on the SF-424 form. For more detailed instructions for obtaining a UEI number, refer to SAM.gov.

Obtain Employer Identification Number:

In addition to having a UEI number, all entities applying for funding must provide an Employer Identification Number (EIN). The EIN can be obtained from the IRS by visiting https://www.irs.gov/businesses/small-businesses-self-employed/apply-for-an-employer-identification-number-ein-online.

Create a login.gov account:

Applicants must have a login.gov account in order to register with SAM or update their SAM registration. Applicants can create a login.gov account at: https://secure.login.gov/sign_up/enter_email?request_id=34f19fa8-14a2-438c-8323-a62b99571fd.

Applicants only have to create a login.gov account once. For existing SAM users, use the same email address for both login.gov and SAM.gov so that the two accounts can be linked.

For more information on the login.gov requirements for SAM registration, refer to https://www.sam.gov/SAM/pages/public/loginFAQ.jsf.

Register with SAM:

In addition to having a UEI number, all organizations must register with SAM. Failure to register with SAM will prevent your organization from applying through FEMA GO. SAM registration must be renewed annually and must remain active throughout the entire grant life cycle.

For more detailed instructions for registering with SAM, refer to: Register with SAM

Note: per 2 C.F.R. § 25.200, applicants must also provide the applicant's immediate and highest-level owner, subsidiaries, and predecessors that have been awarded federal contracts or federal financial assistance within the past three years, if applicable.

Register in FEMA GO, Add the Organization to the System, and Establish the AOR:

Applicants must register in FEMA GO and add their organization to the system. The organization's electronic business point of contact (eBiz POC) from the SAM registration may need to be involved in this step. For step-by-step instructions, see FEMA GO Startup Guide.

Note: FEMA GO will support only the most recent major release of the following browsers:

- Google Chrome;
- Mozilla Firefox;
- Apple Safari; and

- Microsoft Edge.

Applicants using tablet type devices or other browsers may encounter issues with using FEMA GO.

Submitting the Final Application:

Applicants will be prompted to submit the standard application information, and any program-specific information required. Standard Forms (SF) may be accessed in the Forms tab under the SF-424 family on Grants.gov.

Applicants should review these forms before applying to ensure they are providing all required information.

After submitting the final application, FEMA GO will provide either an error message, or an email to the submitting AOR confirming the transmission was successfully received.

B. Application Deadline
08/15/2025 at 05:00 PM Eastern Time

C. Pre-Application Requirements Deadline
Not applicable.

D. Post-Application Requirements Deadline
Not applicable.

E. Effects of Missing the Deadline
All applications must be completed in FEMA GO by the application deadline. FEMA GO automatically records proof of submission and generates an electronic date/time stamp when FEMA GO successfully receives an application. The submitting AOR will receive via email the official date/time stamp and a FEMA GO tracking number to serve as proof of timely submission prior to the application deadline.

Applicants experiencing system-related issues have until 3:00 PM ET on the date applications are due to notify FEMA. No new system-related issues will be addressed after this deadline. Applications not received by the application submission deadline will not be accepted.

6. Intergovernmental Review

A. Requirement Description and State Single Point of Contact
An intergovernmental review may be required. Applicants must contact their state's Single Point of Contact (SPOC) to comply with the state's process under Executive Order 12372.

N/A

7. Application Review Information

A. Threshold Criteria
Applicants must be a Tribal government that is eligible for the program as described in Section 2, "Eligibility." FY 2025 TCGP applications are limited to only those meritorious applicant

projects and investments as identified by FEMA in individual notifications to the eligible Tribal governments.

B. Application Criteria

FEMA will evaluate the FY 2025 TCGP applications for completeness and applicant eligibility. CISA will evaluate the FY 2025 TCGP applications for adherence to programmatic guidelines, and anticipated effectiveness of the proposed investments.

The process for the application criteria, reviews, scoring and ranking used during FY 2022/2023 is described below and informed the selection of FY 2025 TCGP applicants and investments. This information is included here for informational purposes only for FY 2025 TCGP.

For eligible entities with a CISA-approved Cybersecurity Plan, Committee Membership List, and Charter, the review will include verification of the following elements:

a. Eligible entities understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments;
b. Eligible entities implement security protections commensurate with risk; and
c. Eligible entities ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

In addition to the above, CISA will evaluate whether proposed projects are: 1) both feasible and effective at reducing the risks for which the project was designed; and 2) able to be fully completed within the four-year period of performance.

All proposed investments will undergo a federal review by FEMA and CISA to verify compliance with all administrative and eligibility criteria identified in the NOFO. FEMA will conduct the federal review for compliance and the budget review of the IJ(s) and PW. FEMA will use a checklist to verify compliance with all administrative and eligibility criteria identified in the NOFO.

Applicants must demonstrate how investments support closing capability gaps or sustaining capabilities. CISA will review IJ(s) and PW at both the investment and project level. The following criteria apply to the review of projects:

- Clarity: Sufficient detail to understand what the project is intending to do with grant dollars.
- Logical/Project Alignment: Alignment of the stated TCGP objectives to the applicant's approved Cybersecurity Plan.
- Reasonableness: Costs for the items/services outlined within the project description are reasonable. Execution within the period of performance is feasible.

Projects rated as effective or promising are approved.

In addition, investments with emergency communications activities will be reviewed to verify compliance with the SAFECOM Guidance on Emergency Communications Grants. FEMA and

CISA will coordinate directly with the recipient on any compliance concerns and will provide technical assistance as necessary to help ensure full compliance.

The applicant is required to describe its existing capabilities and its proposal to facilitate the successful implementation of this program. For this reason, each application will be evaluated primarily based upon the applicant's method for program implementation. Tribes should demonstrate their understanding of this announcement's objectives and plan for implementing and successfully demonstrating these objectives. In particular, the applicant must address how it meets the eligibility criteria listed in section C of this funding notice and provide evidence demonstrating this eligibility.

If the application fails to address each of the eligibility criteria listed in the above sections, the applicant will be deemed ineligible and will not be considered for an award.

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. To determine eligibility, the FEMA HQ Preparedness Officer will review submitted applications for completeness. Completeness is determined by confirming:
    a. The applicant has submitted the self-certification[5] of eligibility and population section on the IJ Template stating the tribe's eligibility per the *Homeland Security Act of 2002* (see Section C. Eligibility Information, for further information);
    b. The information provided in the self-certification of eligibility and population section on the IJ Template is accurate;
    c. Activities under each investment are allowable; and
    d. The application meets all the administrative criteria identified in this funding notice, to include the required submission of an IJ by the established due dates.
2. CISA is responsible for organizing an objective review panel and establishing the programmatic scoring and selection process. Subject-matter experts on the panel will review and score applications meeting eligibility requirements. The merit review will focus on the overall quality, thoroughness, and completeness of the proposal. The objective review panel will determine whether the proposal addresses the TCGP objectives for the current fiscal year. Scoring is based on the following four IJ sections:
    a. Overview (description of the investment) 5 points;
    b. Baseline (goals/objectives/capabilities of the investment) 5 points;
    c. Project management and milestones (funding amount/core capabilities/projects) 10 points; and
    d. Accomplishments and impacts (outcomes) 5 points.
3. FEMA HQ Grants Management Specialists will conduct a financial review of the top scoring investments using the following criteria:
    a. Allowability, allocability, and financial reasonableness of the proposed budget and investment information; and

b. Whether the recipient meets the financial and legal requirements listed in 2 C.F.R. Part 200.

C. Financial Integrity Criteria

Before making an award, FEMA is required to review OMB-designated databases for applicants' eligibility and financial integrity information. This is required by the Payment Integrity Information Act of 2019 (Pub. L. No. 116-117, § 2 (2020)), 41 U.S.C. § 2313, and the "Do Not Pay Initiative" (31 U.S.C. 3354). For more details, please see 2 C.F.R. § 200.206.

Thus, the Financial Integrity Criteria may include the following risk-based considerations of the applicant:

1. Financial stability.
2. Quality of management systems and ability to meet management standards.
3. History of performance in managing federal award.
4. Reports and findings from audits.
5. Ability to effectively implement statutory, regulatory, or other requirements.

D. Supplemental Financial Integrity Criteria and Review

Before making an award expected to exceed the simplified acquisition threshold (currently a total federal share of $250,000) over the period of performance:

1. FEMA is required by 41 U.S.C. § 2313 to review or consider certain information found in SAM.gov. For details, please see 2 C.F.R. § 200.206(a)(2).
2. An applicant may review and comment on any information in the responsibility/qualification records available in SAM.gov.
3. Before making decisions in the risk review required by 2 C.F.R. § 200.206, FEMA will consider any comments by the applicant.

E. Reviewers and Reviewer Selection

FEMA and CISA Cybersecurity Program staff review all TCGP applications as detailed in Section 7.B above. As an allocated program, there are no additional reviewers or selection processes beyond completeness and eligibility reviews.

FEMA will follow all applicable statutes, rules, and requirements and will take into consideration materials accompanying the TCGP legislation and annual appropriations acts, such as the Joint Explanatory Statement, as appropriate, in reviewing and determining recipient eligibility.

F. Merit Review Process

The only eligible Tribal applicants are those listed in Section 3 of this Notice of Funding Opportunity, "FY 2025 TCGP Allocations," and applications are limited to only those meritorious applicant projects and investments which did not receive funding during the Fiscal Year 2022/2023 award cycle.

G. Final Selection

The only eligible Tribal applicants are those listed in Section 3 of this Notice of Funding Opportunity, "FY 2025 TCGP Allocations," and applications are limited to only those meritorious applicant projects and investments which did not receive funding during the Fiscal

Year 2022/2023 award cycle. All allocations were approved by the Secretary of Homeland Security.

8. Award Notices

A. Notice of Award

The Authorized Organization Representative should carefully read the federal award package before accepting the federal award. The federal award package includes instructions on administering the federal award as well as terms and conditions for the award.

By submitting an application, applicants agree to comply with the prerequisites stated in this NOFO and the material terms and conditions of the federal award, should they receive an award.

FEMA will provide the federal award package to the applicant electronically via FEMA GO. Award packages include an Award Letter, Summary Award Memo, Agreement Articles, and Obligating Document. An award package notification email is sent via the grant application system to the submitting AOR.

Recipients must accept their awards no later than 60 days from the award date. Recipients shall notify FEMA of their intent to accept the award and proceed with work via the FEMA GO system.

Funds will remain on hold until the recipient accepts the award via FEMA GO and all other conditions of the award have been satisfied, or until the award is otherwise rescinded. Failure to accept a grant award within the specified timeframe may result in a loss of funds.

B. Pass-Through Requirements

Not applicable.

C. Note Regarding Pre-Award Costs

Not applicable.

D. Obligation of Funds

Funds are obligated at the time of award. FEMA will provide the federal award package to the applicant electronically via FEMA GO. Award packages include an Award Letter, Summary Award Memo, Agreement Articles, and Obligating Document. An award package notification email is sent via the grant application system to the submitting AOR.

E. Notification to Unsuccessful Applicants

Unsuccessful applicants will be notified electronically through FEMA GO.

9. Post-Award Requirements and Administration

A. Administrative and National Policy Requirements

Presidential Executive Orders

Recipients must comply with the requirements of Presidential Executive Orders related to grants (also known as federal assistance and financial assistance), the full text of which are incorporated by reference.

In accordance with Executive Order 14305, Restoring American Airspace Sovereignty (June 6, 2025), and to the extent allowed by law, eligible state, local, tribal, and territorial grant recipients under this NOFO are permitted to purchase unmanned aircraft systems, otherwise known as drones, or equipment or services for the detection, tracking, or identification of drones and drone signals, consistent with the legal authorities of state, local, tribal, and territorial agencies. Recipients must comply with all applicable federal, state, and local laws and regulations, and adhere to any statutory requirements on the use of federal funds for such unmanned aircraft systems, equipment, or services.

Subrecipient Monitoring and Management
Pass-through entities must comply with the requirements for subrecipient monitoring and management as set forth in 2 C.F.R. §§ 200.331-333.

B. DHS Standard Terms and Conditions
A recipient under this funding opportunity is required to comply with DHS Standard Terms and Conditions in effect as of the date of the federal award. The DHS Standard Terms and Conditions are available online: DHS Standard Terms and Conditions | Homeland Security. For continuation awards, the terms and conditions for the initial federal award will apply unless otherwise specified in the terms and conditions of the continuation award. The specific version of the DHS Standard Terms and Conditions applicable to the federal award will be in the federal award package.

C. Financial Reporting Requirements

1. Recipients must report obligations and expenditures through a federal financial report. The Federal Financial Report (FFR) form, also known as Standard Form 425 (SF-425), is available online at: SF-425 OMB #4040-0014.
2. Recipients must submit the FFR quarterly throughout the period of performance (POP) as detailed below:
3. The final FFR is due within 120 calendar days after the end of the POP.
4. FEMA may withhold future federal awards and cash payments if the recipient does not submit timely financial reports, or the financial reports submitted demonstrate lack of progress or provide insufficient detail.

Reporting Documents	Report Due Date (No Later Than)
October 1 – December 31	January 30
January 1 – March 31	April 30
April 1 – June 30	July 30
July 1 – September 30	October 30
Closeout FFR	No later than 120 days after the end of the POP

D. Programmatic Performance Reporting Requirements

1. A Performance Report must be submitted annually throughout the POP. Recipients should refer to Appendix D, "Sample Performance PPR and Sample Cyber Performance Narrative for Progress Reporting" for the Sample Performance Progress Report (PPR)

and Sample Cyber Performance Narrative for examples of performance metrics and other data necessary to satisfy TCGP programmatic reporting requirements.

2. A Performance Report must include:
    a. Brief narrative of overall project(s) status;
    b. Summary of project expenditures;
    c. Description of any potential issues that may affect project completion;
    d. Data collected for DHS performance measures; and
    e. The report must be signed by the Authorized Official or Signatory Authority.
3. The Progress Report must be submitted through FEMA GO.
4. Performance Report Due Dates
    a. The annual PPR submission is due Jan. 30 of each year to account for the previous calendar year.

E. Closeout Reporting Requirements

Within 120 days after the end of the period of performance, or after an amendment has been issued to close out a federal award, recipients must submit the following:

1. The final request for payment, if applicable.
2. The final FFR.
3. The final progress report detailing all accomplishments.
4. A qualitative narrative summary of the impact of those accomplishments throughout the period of performance.
5. Other documents required by this NOFO, terms and conditions of the federal award, or other DHS Component guidance.

After FEMA approves these reports, it will issue a closeout notice. The notice will indicate the period of performance as closed, list any remaining funds to be de-obligated, and address the record maintenance requirement. Unless a longer period applies, such as due to an audit or litigation, for equipment or real property used beyond the period of performance, or due to other circumstances outlined in 2 C.F.R. § 200.334, this maintenance requirement is three years from the date of the final FFR.

Also, pass-through entities are responsible for closing out those subawards as described in 2 C.F.R. § 200.344; subrecipients are still required to submit closeout materials within 90 calendar days of the subaward period of performance end date. When a subrecipient completes all closeout requirements, pass-through entities must promptly complete all closeout actions in time for the recipient to submit all necessary documentation and information to FEMA during the closeout of their prime award. The recipient is responsible for returning any balances of unobligated or unliquidated funds that have been drawn down that are not authorized to be retained per 2 C.F.R. § 200.344(e).

Administrative Closeout

Administrative closeout is a mechanism for FEMA to unilaterally execute closeout of an award. FEMA will use available award information in lieu of final recipient reports, per 2 C.F.R. § 200.344(h)-(i). It is an activity of last resort, and if FEMA administratively closes an award, this may negatively impact a recipient's ability to obtain future funding.

Additional Reporting Requirements
Recipients and subrecipients are required to adhere to all deadlines detailed in this NOFO as described in Appendix A, "TCGP Requirements Matrix."

F. Disclosing Information per 2 C.F.R. § 180.335

Before entering into a federal award, the applicant must notify FEMA if it knows that the applicant or any of the principals (as defined at 2 C.F.R. § 180.995) for the federal award:

1. Are presently excluded or disqualified;
2. Have been convicted within the preceding three years of any of the offenses listed in § 180.800(a) or had a civil judgment rendered against you for one of those offenses within that time period;
3. Are presently indicted for or otherwise criminally or civilly charged by a governmental entity (Federal, State, or local) with the commission of any of the offenses listed in § 180.800(a); or
4. Have had one or more public transactions (Federal, State, or local) terminated within the preceding three years for cause or default.

This is requirement is fully described in 2 C.F.R. §180.335.

Additionally, 2 C.F.R. § 180.350 requires recipients to provide immediate notice to FEMA at any time after entering a federal award if:

1. The recipient learns that either it failed to earlier disclose information as required by 2 C.F.R. § 180.335;
2. Due to changed circumstances, the applicant or any of the principals for the federal award now meet the criteria at 2 C.F.R. § 180.335 listed above.

G. Reporting of Matters Related to Recipient Integrity and Performance

Appendix XII to 2 C.F.R. Part 200 states the terms and conditions for recipient integrity and performance matters used for this funding opportunity.

If the total value of all active federal grants, cooperative agreements, and procurement contracts for a recipient exceeds $10,000,000 at any time during the period of performance:

1. The recipient must maintain the currency of information reported in SAM.gov about civil, criminal, or administrative proceedings described in paragraph 2 of Appendix XII;
2. The required reporting frequency is described in paragraph 4 of Appendix XII.

H. Single Audit Report

A recipient expending $1,000,000 or more in federal awards (as defined by 2 C.F.R. § 200.1) during its fiscal year must undergo an audit. This may be either a single audit complying with 2 C.F.R. § 200.514 or a program-specific audit complying with 2 C.F.R. §§ 200.501 and 200.507. Audits must follow 2 C.F.R. Part 200, Subpart F, 2 C.F.R. § 200.501, and the U.S. Government Accountability Office (GAO) Generally Accepted Government Auditing Standards.

I. Monitoring and Oversight

Per 2 C.F.R. § 200.337, DHS and its authorized representatives have the right of access to any records of the recipient or subrecipient pertinent to a Federal award to perform audits, site visits, and any other official use. The right also includes timely and reasonable access to the recipient's

or subrecipient's personnel for the purpose of interview and discussion related to such documents or the Federal award in general.

Pursuant to this right and per 2 C.F.R. § 200.329, DHS may conduct desk reviews and make site visits to review and evaluate project accomplishments and management control systems as well as provide any required technical assistance. Recipients and subrecipients must respond in a timely and accurate manner to DHS requests for information relating to a federal award.

Recipients and subrecipients who are pass-through entities are responsible for monitoring their subrecipients in a manner consistent with the terms of the federal award at 2 C.F.R. Part 200, including 2 C.F.R. § 200.332. This includes the pass-through entity's responsibility to monitor the activities of the subrecipient as necessary to ensure that the subaward is used for authorized purposes, in compliance with federal statutes, regulations, and the terms and conditions of the subaward; and that subaward performance goals are achieved.

In terms of overall award management, recipient and subrecipient responsibilities include, but are not limited to: accounting of receipts and expenditures, cash management, maintaining adequate financial records, reporting and refunding expenditures disallowed by audits, monitoring if acting as a pass-through entity, or other assessments and reviews, and ensuring overall compliance with the terms and conditions of the award or subaward, as applicable, including the terms of 2 C.F.R. Part 200.

J. Program Evaluation

Title I of the Foundations for Evidence-Based Policymaking Act of 2018, Pub. L. No. 115-435 (2019) (Evidence Act) urges federal agencies to use program evaluation as a critical tool to learn, improve delivery, and elevate program service and delivery across the program lifecycle. Evaluation means "an assessment using systematic data collection and analysis of one or more programs, policies, and organizations intended to assess their effectiveness and efficiency." Evidence Act, § 101 (codified at 5 U.S.C. § 311). OMB A-11, Section 290 (Evaluation and Evidence-Building Activities) further outlines the standards and practices for evaluation activities. Federal agencies are required to specify any requirements for recipient participation in program evaluation activities (2 C.F.R. § 200.301). Program evaluation activities incorporated from the outset in the NOFO and program design and implementation allow recipients and agencies to meaningfully document and measure progress and achievement towards program goals and objectives, and identify program outcomes and lessons learned, as part of demonstrating recipient performance (2 C.F.R. § 200.301).

As such, recipients and subrecipients are required to participate in a Program Office (PO) or a DHS Component-led evaluation, if selected. This may be carried out by a third-party on behalf of the PO or the DHS Component. Such an evaluation may involve information collections including but not limited to, records of the recipients; surveys, interviews, or discussions with individuals who benefit from the federal award, program operating personnel, and award recipients; and site visits or other observation of recipient activities, as specified in a DHS Component or PO-approved evaluation plan. More details about evaluation requirements may be provided in the federal award, if available at that time, or following the award as evaluation requirements are finalized. Evaluation costs incurred during the period of performance are allowable costs (either as direct or indirect) in accordance with 2 C.F.R.§ 200.413. Recipients and subrecipients are also encouraged, but not required, to participate in any additional

evaluations after the period of performance ends, although any costs incurred to participate in such evaluations are not allowable and may not be charged to the federal award.

K. Additional Performance Reporting Requirements
Not applicable.

L. Termination of the Federal Award by FEMA

1. Paragraph C.XL of the FY 2025 DHS Standard Terms and Conditions, v.3 sets forth a term and condition entitled "Termination of a Federal Award." The termination provision condition listed below applies to the grant award and the term and condition in Paragraph C.XL of the FY 2025 DHS Standard Terms and Conditions, v.3 does not**.**

2. Termination of the Federal Award by FEMA

   FEMA may terminate the federal award in whole or in part for one of the following reasons identified in 2 C.F.R. § 200.340:

   a. If the recipient or subrecipient fails to comply with the terms and conditions of the federal award.

   b. With the consent of the recipient, in which case FEMA and the recipient must agree upon the termination conditions. These conditions include the effective date and, in the case of partial termination, the portion to be terminated.

   c. If the federal award no longer effectuates the program goals or agency priorities. Under this provision, FEMA may terminate the award for these purposes if any of the following reasons apply:

      i. If DHS/FEMA, in its sole discretion, determines that a specific award objective is ineffective at achieving program goals as described in this NOFO;

      ii. If DHS/FEMA, in its sole discretion, determines that an objective of the award as described in this NOFO will be ineffective at achieving program goals or agency priorities;

      iii. If DHS/FEMA, in its sole discretion, determines that the design of the grant program is flawed relative to program goals or agency priorities;

      iv. If DHS/FEMA, in its sole discretion, determines that the grant program is not aligned to either the DHS Strategic Plan, the FEMA Strategic Plan, or successor policies or documents;

      v. If DHS/FEMA, in its sole discretion, changes or re-evaluates the goals or priorities of the grant program and determines that the award will be ineffective at achieving the updated program goals or agency priorities; or

      vi. For other reasons based on program goals or agency priorities described in the termination notice provided to the recipient pursuant to 2 C.F.R. § 200.341.

vii. If the awardee falls out of compliance with the Agency's statutory or regulatory authority, award terms and conditions, or other applicable laws.

3. Termination of a Subaward by the Pass-Through Entity

   The pass-through entity may terminate a subaward in whole or in part for one of the following reasons identified in 2 C.F.R. § 200.340:

   a. If the subrecipient fails to comply with the terms and conditions of the federal award.

   b. With the consent of the subrecipient, in which case the pass-through entity and the subrecipient must agree upon the termination conditions. These conditions include the effective date and, in the case of partial termination, the portion to be terminated.

   c. If the pass-through entity's award has been terminated, the pass-through recipient will terminate its subawards.

4. Termination by the Recipient or Subrecipient

   The recipient or subrecipient may terminate the federal award in whole or in part for the following reason identified in 2 C.F.R. § 200.340: Upon sending FEMA or the pass-through entity a written notification of the reasons for such termination, the effective date, and, in the case of partial termination, the portion to be terminated. However, if FEMA or the pass-through entity determines that the remaining portion of the federal award will not accomplish the purposes for which the federal award was made, FEMA or the pass-through entity may terminate the federal award in its entirety.

5. Impacts of Termination

   a. When FEMA terminates the federal award prior to the end of the period of performance due to the recipient's material failure to comply with the terms and conditions of the federal award, FEMA will report the termination in SAM.gov in the manner described at 2 C.F.R. § 200.340(c).

   b. When the federal award is terminated in part or its entirety, FEMA or the pass-through entity and recipient or subrecipient remain responsible for compliance with the requirements in 2 C.F.R. §§ 200.344 and 200.345.

6. Notification Requirements

   FEMA or the pass-through entity must provide written notice of the termination in a manner consistent with 2 C.F.R. § 200.341. The federal award will be terminated on the date of the notification unless stated otherwise in the notification.

7. Opportunities to Object and Appeals

Where applicable, when FEMA terminates the federal award, the written notification of termination will provide the opportunity, and describe the process, to object and provide information challenging the action, pursuant to 2 C.F.R. § 200.342.

8. Effects of Suspension and Termination

   The allowability of costs to the recipient or subrecipient resulting from financial obligations incurred by the recipient or subrecipient during a suspension or after the termination of a federal award are subject to 2 C.F.R. § 200.343.

M. Best Practice

While not a requirement in the DHS Standard Terms and Conditions, as a best practice, entities receiving funds through this program should ensure that cybersecurity is integrated into the design, development, operation, and maintenance of investments that impact information technology (IT) and/ or operational technology (OT) systems. Additionally, "The recipient and subrecipient must … take reasonable cybersecurity and other measures to safeguard information including protected personally identifiable information (PII) and other types of information." 2 C.F.R. § 200.303(e).

N. Payment Information

Recipients will submit payment requests in FEMA GO for FY25 awards under this program.

Instructions to Grant Recipients Pursuing Payments

FEMA reviews all grant payments and obligations to ensure allowability in accordance with 2 C.F.R. § 200.305. These measures ensure funds are disbursed appropriately while continuing to support and prioritize communities who rely on FEMA for assistance. Once a recipient submits a payment request in FEMA GO, FEMA will review the request. If FEMA approves a payment, recipients will be notified by FEMA GO and the payment will be delivered pursuant to the recipients SAM.gov financial information. If FEMA disapproves a payment, FEMA will inform the recipient.

Processing and Payment Timeline

FEMA must comply with regulations governing payments to grant recipients. See 2 C.F.R. § 200.305. For grant recipients other than States, 2 C.F.R. § 200.305(b)(3) stipulates that FEMA is to make payments on a reimbursement basis within 30 days after receipt of the payment request, unless FEMA reasonably believes the request to be improper. For state recipients, 2 C.F.R. § 200.305(a) instructs that federal grant payments are governed by Treasury-State Cash Management Improvement Act agreements ("Treasury-State agreement") and default procedures codified at 31 C.F.R. Part 205 and Treasury Financial Manual 4A-2000, "Overall Disbursing Rules for All Federal Agencies." *See* 2 C.F.R. § 200.305(a).

Treasury-State agreements generally apply to "major federal assistance programs" that are governed by 31 C.F.R. Part 205, subpart A and are identified in the Treasury-State agreement. 31 C.F.R. §§ 205.2, 205.6. Where a federal assistance (grant) program is not governed by subpart A, payment and funds transfers from FEMA to the state are subject to 31 C.F.R. Part 205, subpart B. Subpart B requires FEMA to "limit a funds transfer to a state to the minimum amounts needed by the state and must time the disbursement to be in accord with the actual, immediate cash

requirements of the state in carrying out a federal assistance program or project. The timing and amount of funds transfers must be as close as is administratively feasible to a state's actual cash outlay for direct program costs and the proportionate share of any allowable indirect costs." 31 C.F.R. § 205.33(a). Nearly all FEMA grants are not "major federal assistance programs." As a result, payments to states for those grants are subject to the "default" rules of 31 C.F.R. Part 205, subpart B.

If additional information is needed, a request for information will be issued by FEMA to the recipient; recipients are strongly encouraged to respond to any additional request for information inquiries within three business days. If an adequate response is not received, the request may be denied, and the entity may need to submit a new reimbursement request; this will re-start the 30-day timeline.

Submission Process
All non-disaster grant program reimbursement requests must be reviewed and approved by FEMA prior to drawdowns.

For all non-disaster reimbursement requests (regardless of system), please submit the following information:

1. Grant ID / Award Number
2. Total amount requested for drawdown
3. Purpose of drawdown and timeframe covered (must be within the award performance period)
4. Subrecipient Funding Details (if applicable)

- Is funding provided directly or indirectly to a subrecipient?
  - If **no,** include statement "This grant funding is not being directed to a subrecipient."
- If **yes**, provide the following details:
  - The name, mission statement, and purpose of each subrecipient receiving funds, along with the amount allocated and the specific role or activity being reimbursed.
  - Whether the subrecipient work or mission involves supporting aliens, regardless of whether FEMA funds support such activities.
  - Whether the payment request includes an activity involving support to aliens.
  - Whether the subrecipient has any diversity, equity, and inclusion practices.

5. Supporting documentation to demonstrate that expenses are allowable, allocable, reasonable, and necessary under 2 C.F.R. Part 200 and in compliance with the grant's NOFO, award terms, and applicable federal regulations.

O. Immigration Conditions
A recipient under this funding opportunity must comply with the FY 2025 Department of Homeland Security Standard Terms and Conditions, v. 3 (Apr. 18, 2025), with the exception Paragraph C.IX (Communication and Cooperation with the Department of Homeland Security and Immigration Officials) and paragraph C.XVII(2)(a)(iii) (Anti-Discrimination Grant Award Certification regarding immigration). Paragraphs C.IX and C.XVII(2)(a)(iii) do not apply to any federal award under this funding opportunity. The FY 2025 Department of Homeland Security Standard Terms and Conditions, v. 3 (Apr. 18, 2025) are available at www.dhs.gov/publication/dhs-standard-terms-and-conditions.

10. Other Information

A. Period of Performance Extension

Extensions to the period of performance (POP) are not allowed.

B. Other Information

a. *Environmental Planning and Historic Preservation (EHP) Compliance*

The federal government is required to consider effects of its actions on the environment and historic properties to ensure that activities, grants, and programs funded by FEMA, comply with federal EHP laws, Executive Orders, regulations, and policies.

Recipients and subrecipients proposing projects with the potential to impact the environment or cultural resources, such as the modification or renovation of existing buildings, structures, and facilities, and/or new construction and/or replacement of buildings, structures, and facilities, must participate in the FEMA EHP review process. This includes conducting early engagement to help identify EHP resources, such as threatened or endangered species, historic properties, or communities with environmental concerns; submitting a detailed project description with supporting documentation to determine whether the proposed project has the potential to impact EHP resources; and, identifying mitigation measures and/or alternative courses of action that may lessen impacts to those resources.

FEMA is sometimes required to consult with other regulatory agencies and the public in order to complete the review process. Federal law requires EHP review to be completed before federal funds are released to carry out proposed projects. FEMA may not be able to fund projects that are not in compliance with applicable EHP laws, Executive Orders, regulations, and policies. FEMA may recommend mitigation measures and/or alternative courses of action to lessen impacts to EHP resources and bring the project into EHP compliance.

EHP guidance is found at Environmental Planning and Historic Preservation. The site contains links to documents identifying agency EHP responsibilities and program requirements, such as implementation of the National Environmental Policy Act and other EHP laws, regulations, and Executive Orders. DHS and FEMA EHP policy is also found in the EHP Directive & Instruction.

All FEMA actions, including grants, must comply with National Flood Insurance Program (NFIP) criteria or any more restrictive federal, state, or local floodplain management standards or building code (44 C.F.R. § 9.11(d)(6)). For actions located within or that may affect a floodplain or wetland, the following alternatives must be considered: a) no action; b) alternative locations; and c) alternative actions, including alternative actions that use natural features or nature-based solutions. Where possible, natural features and nature-based solutions shall be used. If not practicable as an alternative on their own, natural features and nature-based solutions may be incorporated into actions as minimization measures.

The GPD EHP screening form is located at https://www.fema.gov/sites/default/files/documents/fema_ehp-screening_form_ff-207-fy-21-100_5-26-2021.pdf.

b. *Procurement Integrity*

When purchasing under a FEMA award, recipients and subrecipients must comply with the federal procurement standards in 2 C.F.R. §§ 200.317 – 200.327. To assist with determining whether an action is a procurement or instead a subaward, please consult 2 C.F.R. § 200.331. For detailed guidance on the federal procurement standards, recipients and subrecipients should refer to various materials issued by FEMA's Procurement Disaster Assistance Team (PDAT). Additional resources, including an upcoming trainings schedule can be found on the PDAT Website: https://www.fema.gov/grants/procurement.

Under 2 C.F.R. § 200.317, when procuring property and services under a federal award, States (including territories) and Indian Tribes, must follow the same policies and procedures they use for procurements from their non-federal funds; additionally, states and Indian Tribes must now follow 2CFR § 200.322 regarding domestic preferences for Procurements and 2 C.F.R. § 200.327 regarding required contract provisions. States, but not Indian Tribes, must also follow 2 C.F.R. § 200.323 regarding procurement of recovered materials.

Local government and nonprofit recipients or subrecipients must have and use their own documented procurement procedures that reflect applicable SLTT laws and regulations, provided that the procurements conform to applicable federal law and the standards identified in 2 C.F.R. Part 200.

Important Changes to Procurement Standards in 2 C.F.R. Part 200

On April 22, 2024, OMB updated various parts of Title 2 of the Code of Federal Regulations, among them the procurement standards. These revisions apply to all FEMA awards with a federal award date or disaster declaration date on or after October 1, 2024, unless specified otherwise. The changes include updates to the federal procurement standards, which govern how FEMA award recipients and subrecipients must purchase under a FEMA award.

More information on OMB's revisions to the federal procurement standards can be found in Purchasing Under a FEMA Award: 2024 OMB Revisions Fact Sheet.

Competition and Conflicts of Interest

2 C.F.R. § 200.319(b), applicable to local government and nonprofit recipients or subrecipients, requires that contractors that develop or draft specifications, requirements statements of work, or invitations for bids or requests for proposals must be excluded from competing for such procurements. FEMA considers these actions to be an organizational conflict of interest and interprets this restriction as applying to contractors that help a recipient or subrecipient develop its grant application, project plans, or project budget. This prohibition also applies to the use of former employees to manage the grant or carry out a contract when those former employees worked on such activities while they were employees of the recipient or subrecipient.

Under this prohibition, unless the recipient or subrecipient solicits for and awards a contract covering both development and execution of specifications (or similar elements as described above), and this contract was procured in compliance with 2 C.F.R. §§ 200.317 – 200.327, federal funds cannot be used to pay a contractor to carry out the work if that contractor also worked on the development of those specifications. This rule applies to all contracts funded with

federal grant funds, including pre-award costs, such as grant writer fees, as well as post- award costs, such as grant management fees.

In addition to organizational conflicts of interest, situations considered to be restrictive of competition include, but are not limited to:

- Placing unreasonable requirements on firms for them to qualify to do business;
- Requiring unnecessary experience and excessive bonding;
- Noncompetitive pricing practices between firms or between affiliated companies;
- Noncompetitive contracts to consultants that are on retainer contracts;
- Specifying only a "brand name" product instead of allowing "an equal" product to be offered and describing the performance or other relevant requirements of the procurement; and
- Any arbitrary action in the procurement process.

Under 2 C.F.R. § 200.318(c)(1), local government and nonprofit recipients or subrecipients are required to maintain written standards of conduct covering conflicts of interest and governing the actions of their employees engaged in the selection, award, and administration of contracts. No employee, officer, or agent may participate in the selection, award, or administration of a contract supported by a federal award if he or she has a real or apparent conflict of interest. Such conflicts of interest would arise when the employee, officer or agent, any member of his or her immediate family, his or her partner, or an organization that employs or is about to employ any of the parties indicated herein, has a financial or other interest in or a tangible personal benefit from a firm considered for a contract. The officers, employees, and agents of the recipient or subrecipient may neither solicit nor accept gratuities, favors, or anything of monetary value from contractors or parties to subcontracts. However, the recipient or subrecipient may set standards for situations in which the financial interest is not substantial, or the gift is an unsolicited item of nominal value. The recipient's or subrecipient's standards of conduct must provide for disciplinary actions to be applied for violations of such standards by officers, employees, or agents.

Under 2 C.F.R. § 200.318(c)(2), if the local government and nonprofit recipient or subrecipient has a parent, affiliate, or subsidiary organization that is not a SLTT government, the recipient or subrecipient must also maintain written standards of conduct covering organizational conflicts of interest. Organizational conflict of interest means that because of a relationship with a parent company, affiliate, or subsidiary organization, the recipient or subrecipient is unable or appears to be unable to be impartial in conducting a procurement action involving a related organization. The recipient or subrecipient must disclose in writing any potential conflicts of interest to FEMA or the pass-through entity in accordance with applicable FEMA policy.

Supply Schedules and Purchasing Programs

Generally, a recipient or subrecipient may seek to procure goods or services from a federal supply schedule, state supply schedule, or group purchasing agreement.

Information about GSA programs for states, Indian Tribes, and local governments, and their instrumentalities, can be found at Purchasing Resources and Support for State and Local Governments.pdf

Help for state, local, and tribal governments to make MAS buys | GSA and https://www.gsa.gov/buying-selling/purchasing- programs/gsa-schedules/schedule-buyers/state-and-local-governments.

Procurement Documentation

Per 2 C.F.R. § 200.318(i), local government and nonprofit recipients or subrecipients are required to maintain and retain records sufficient to detail the history of procurement covering at least the rationale for the procurement method, selection of contract type, contractor selection or rejection, and the basis for the contract price. States and Indian Tribes are reminded that in order for any cost to be allowable, it must be adequately documented per 2 C.F.R. § 200.403(g).

Examples of the types of documents that would cover this information include but are not limited to:

- Solicitation documentation, such as requests for quotes, invitations for bids, or requests for proposals;
- Responses to solicitations, such as quotes, bids, or proposals;
- Pre-solicitation independent cost estimates and post-solicitation cost/price analyses on file for review by federal personnel, if applicable;
- Contract documents and amendments, including required contract provisions; and
- Other documents required by federal regulations applicable at the time a grant is awarded to a recipient.

c. *Financial Assistance Programs for Infrastructure*

Recipients and subrecipients must comply with FEMA's implementation requirements of the Build America, Buy America Act (BABAA), which was enacted as part of the Infrastructure Investment and Jobs Act §§ 70901-70927, Pub. L. No. 117-58 (2021); and Executive Order 14005, Ensuring the Future is Made in All of America by All of America's Workers. See also 2 C.F.R. Part 184, Buy America Preferences for Infrastructure Projects and OMB Memorandum M-24-02, Implementation Guidance on Application of Buy America Preference in Federal Financial Assistance Programs for Infrastructure.

None of the funds provided under this program may be used for a project for infrastructure unless the iron and steel, manufactured products, and construction materials used in that infrastructure are produced in the United States.

The Buy America preference only applies to articles, materials, and supplies that are consumed in, incorporated into, or affixed to an infrastructure project. As such, it does not apply to tools, equipment, and supplies, such as temporary scaffolding, brought to the construction site and removed at or before the completion of the infrastructure project. Nor does a Buy America preference apply to equipment and furnishings, such as movable chairs, desks, and portable computer equipment, that are used at or within the finished infrastructure project but are not an integral part of the structure or permanently affixed to the infrastructure project.

To see whether a particular FEMA federal financial assistance program is considered an infrastructure program and thus required to implement FEMA's Build America, Buy America

requirements, please see Programs and Definitions: Build America, Buy America Act | FEMA.gov.

Waivers

When necessary, recipients (and subrecipients through their pass-through entity) may apply for, and FEMA may grant, a waiver from these requirements.

A waiver of the domestic content procurement preference may be granted by the agency awarding official if FEMA determines that:

- Applying the domestic content procurement preference would be inconsistent with the public interest, or
- The types of iron, steel, manufactured products, or construction materials are not produced in the United States in sufficient and reasonably available quantities or of a satisfactory quality, or
- The inclusion of iron, steel, manufactured products, or construction materials produced in the United States will increase the cost of the overall project by more than 25%.

The process for requesting a waiver from the Buy America preference requirements can be found on FEMA's website at: "Buy America" Preference in FEMA Financial Assistance Programs for Infrastructure | FEMA.gov.

Definitions

For definitions of the key terms of the Build America, Buy America Act, please visit Programs and Definitions: Build America, Buy America Act | FEMA.gov.

d. *Mandatory Disclosures*

The non-Federal entity or applicant for a federal award must disclose, in a timely manner, in writing to the federal awarding agency or pass-through entity all violations of federal criminal law involving fraud, bribery, or gratuity violations potentially affecting the Federal award, 2 C.F.R. § 200.113.

f. *Adaptive Support*

Pursuant to Section 504 of the Rehabilitation Act of 1973, recipients of FEMA financial assistance must ensure that their programs and activities do not discriminate against qualified individuals with disabilities.

g. *Record Retention*

Record Retention Period

Financial records, supporting documents, statistical records, and all other non-Federal entity records pertinent to a Federal award generally must be maintained for at least three years from the date the final FFR is submitted. *See* 2 C.F.R. § 200.334. Further, if the recipient does not

submit a final FFR and the award is administratively closed, FEMA uses the date of administrative closeout as the start of the general record retention period.

The record retention period **may be longer than three years or have a different start date** in certain cases.

Types of Records to Retain

FEMA requires that recipients and subrecipients maintain the following documentation for federally funded purchases:

- Specifications
- Solicitations
- Competitive quotes or proposals
- Basis for selection decisions
- Purchase orders
- Contracts
- Invoices
- Cancelled checks

h. ***Actions to Address Noncompliance***

Non-federal entities receiving financial assistance funding from FEMA are required to comply with requirements in the terms and conditions of their awards or subawards, including the terms set forth in applicable federal statutes, regulations, NOFOs, and policies. Throughout the award lifecycle or even after an award has been closed, FEMA or the pass-through entity may discover potential or actual noncompliance on the part of a recipient or subrecipient.

In the case of any potential or actual noncompliance, FEMA may place special conditions on an award per 2 C.F.R. §§ 200.208 and 200.339. FEMA may place a hold on funds until the matter is corrected, or additional information is provided per 2 C.F.R. § 200.339, or it may do both. Similar remedies for noncompliance with certain federal civil rights laws are authorized pursuant to 44 C.F.R. Part 7 and 44 C.F.R. Part 44 C.F.R. Part 19 or other applicable regulations.

If the noncompliance is not able to be corrected by imposing additional conditions or the recipient or subrecipient refuses to correct the matter, FEMA may take other remedies allowed under 2 C.F.R. § 200.339.

i. ***Audits***

FEMA grant recipients are subject to audit oversight from multiple entities including the DHS OIG, the GAO, the pass-through entity, or independent auditing firms for single audits, and may cover activities and costs incurred under the award. Auditing agencies such as the DHS OIG, the GAO, and the pass-through entity (if applicable), and FEMA in its oversight capacity, must have access to records pertaining to the FEMA award.

11. Appendix A: TCGP Requirements Matrix

ID	Category	Requirement	Location	Due Date Cycle	Due Date	Submission Plan
1	Post-Award	Cybersecurity Plan or Cybersecurity Plan Template	NOFO Sec 3	Prior to award or during POP (if not already approved by CISA)	Varies	Post Award: FEMA GO
2	Post-Award	Cybersecurity Planning Committee Membership List	NOFO Sec 3	Prior to award (or during POP (if not already approved by CISA)	Varies	Post Award: FEMA GO
3	Post-Award	Cybersecurity Planning Committee Charter	NOFO Sec 3	Prior to award or during POP (if not already approved by CISA)	Varies	Post Award: FEMA GO
4	Post-Award	Investment Justification (IJ)	NOFO Sec 4	Prior to award	Varies	Post Award: FEMA GO
5	Post-Award	Project Worksheet (PW)	NOFO Sec 4	Prior to award	Varies	Prior to Award: FEMA GO
6	Closeout	Closeout Reporting Requirements	NOFO Sec 9	Within 120 days after end of POP	Varies	Submit final SF-425 Federal Financial Report (FFR) in PARS; and process final reimbursement requests in PARS
7	Exercises	EHP review/approval	NOFO Sec 10	Prior to conducting exercises that require EHP Review as outlined in NOFO Section F.	Varies	Email to: GPDEHPInfo@fema.dhs.gov and cc: FEMA-TCGP@fema.dhs.gov
8	Reporting	Standard Form (SF) 425, also known as the Federal Financial Report (FFR)	NOFO Sec 9	Quarterly	30-Jan 30-Apr 30-Jul 30-Oct	Submit SF-425 FFR in Payment and Reporting Systems (PARS)
9	Progress Reporting and Performance Measurement	Performance Progress Report (PPR)	NOFO Sec 9	Once annually and at Closeout	30-Jan and Closeout	Submit Signed PPR (pdf) in FEMA GO
10	Reporting	Single Audit Report	NOFO Sec 9	Throughout POP	Varies	Federal Audit Clearinghouse https://facweb.census.gov/uploadpdf.aspx

16. Appendix B: Post-Award Program-specific Required Documents, Forms and Information

The following program-specific forms or information are required to be submitted in FEMA GO after awards are made:

1. Cybersecurity Project Submissions
   a. Investment Justifications
   b. Project Worksheets (FEMA will provide recipients with a draft Project Worksheet, including the 40% required Cost Share)
   c. Detailed Budget Worksheet and Narrative (Appendix E, "Sample Budget Worksheet and Budget Narrative")
   d. Negotiated Indirect Cost Rate Agreement (if applicable)
2. Cybersecurity Planning Committee Membership List and Charter
3. Cybersecurity Plan with required signatures (resubmissions of updated plan, if applicable)
4. SF-424A, Budget Information (Non-Construction) (as an attachment in FEMA GO)

All Cost Share Waiver requests must be submitted post-award by the eligible entity by emailing the request and supporting documentation (refer to section 2.G. Cost Sharing Requirement) to FEMA-TCGP@fema.dhs.gov.

All program-specific forms are available on Grants.gov and Tribal Cybersecurity Grant Program | FEMA.gov. Recipients can email questions about program-specific required documents, forms and information to FEMA-TCGP@fema.dhs.gov. User guides are available for TCGP IJs and PWs at Tribal Cybersecurity Grant Program | FEMA.gov. Additional programmatic guidance can be found at https://www.cisa.gov/cybergrants/tcgp.

The following descriptions detail instructions for each required program-specific document post award.

1. Cybersecurity Project Submission

a. Investment Justification (IJ) Template and Instructions

Each eligible tribe is required to submit completed project-level information detailing how the TCGP program objectives and goals will be met through the development, implementation, and/or revision of its Cybersecurity Plan. The tribal government must establish a Cybersecurity Planning Committee to approve the signed Cybersecurity Plan submitted post-award in FEMA GO. FY 2025 TCGP applications are limited to only those meritorious applicant projects and investments as identified by FEMA in individual notifications to the eligible Tribal governments. Project-level information should also address the requirement to conduct assessments and evaluation and to incorporate the adoption of key cybersecurity best practices. Tribal governments should consult the CISA Cybersecurity Performance Goals during the development of plans, investments, and project for their TCGP application.

The IJ Template is useful for the **Program Narrative**. All IJs must provide a baseline understanding of the existing cybersecurity gaps, risks, and threats that the recipient faces

which have influenced the development of the IJs. Also, recipients must include a summary of the current capabilities within their jurisdiction to address these threats and risks. For each investment and objective listed on the draft PW provided by FEMA, the recipient must submit a separate IJ form. **Recipients should not include more than one investment and objective per IJ form.**

b. Project Worksheet, Detailed Budget Worksheet and Narrative, Negotiated Indirect Cost Rate Agreement

The **PW** must include information for each IJ submitted for funding. The PW, Budget Worksheet and Budget Narrative should be used to record all proposed projects with budget details, budget narrative, Management and Administrative (M&A) costs, amount and source of the cost share, etc. The Planning, Organization, Equipment, Training, and/or Exercises (POETE) Solution Areas associated with each IJ, and objective must be indicated on the PW.

Note: Please keep in mind that the Federal Amount and required project-based Cost Share Amount must be included for each investment and associated objective within the PW, as well as the Budget Worksheet and Budget Narrative.

The PW, **Budget Worksheet and Budget Narrative** are useful for the Budget Details. The Budget Worksheet and Budget Narrative justifies the need for each budget line item and justifies the cost estimates. The Budget Worksheet and Budget Narrative should include the per unit cost for each item and the quantity requested. The Budget Worksheet and Budget Narrative also explains how the cost(s) relate to the programmatic goals of each investment. Eligible recipients must submit one PW and a separate Budget Worksheet and Budget Narrative, found in Appendix E, "Sample Budget Worksheet and Budget Narrative" as part of the overall post award submission through the FEMA GO system. FY 2025 TCGP applications are limited to only those meritorious applicant projects and investments as identified by FEMA in individual notifications to the eligible Tribal governments.

- FEMA will provide recipients with a draft PW which includes the investment(s) name and number and associated federal amount(s).
- Recipients will use the draft PW as the basis for preparing their IJs and finalizing their PW for submission in FEMA GO.
- For each investment and objective listed on the draft PW provided by FEMA, the recipient must submit a separate IJ form.
- Recipient should use the Sample Budget Worksheet and Budget Narrative in Appendix E, "Sample Budget Worksheet and Budget Narrative" to create and submit their final Budget Worksheet and Budget Narrative as an attachment for submission in FEMA GO. Each cost from the PW must be included on the Budget Worksheet and Budget Narrative
- Recipients should not include more than one investment per IJ form.
- Only the investment(s) and associated IJ funding amount(s) on the draft PW are eligible for project funding with FY 2025 TCGP funding.
- M&A costs must be a separate line item from indirect costs on the PW. To request M&A costs, recipients will need to reduce their investment funding amount(s) on the PW and IJ to account for the M&A funding amounts.

- To request indirect costs, recipients will need to reduce their investment funding amount(s) on the PW and IJ to account for the indirect funding amounts. Requests for indirect costs should include an unexpired, signed **Negotiated Indirect Cost Rate Plan** as an attachment in FEMA GO.

The PW provides drop-down selections for several of the project attributes. All project attribute fields must be completed for the PW to be considered complete in FEMA GO. FEMA and CISA will not review incomplete PWs. Information provided should primarily align to one objective to facilitate project review. If a project aligns to multiple objectives, then the recipient must provide sufficient detail to determine which projects, POETE elements, and requested funds belong under which objective. The recipient may then use the information collected in the worksheet for rapid transfer to the FEMA GO interface. Each project will be given a unique identifier as it is submitted via FEMA GO. Recipients should keep a record of the project identifiers as they will be required to report on each project using that identifier. All requested funding must be associated with specific projects.

2. **Cybersecurity Planning Committee Membership List and Charter**
   All Cybersecurity Planning Committee Membership Lists and Charters must be signed at time of submission via FEMA GO. Additional programmatic guidance can be found at https://www.cisa.gov/cybergrants/tcgp.

   Recipients can contact their CISA grant program staff and regional staff for more information by email at TCGPinfo@mail.cisa.dhs.gov.

3. **Cybersecurity Plan or Cybersecurity Plan Template**
   Section 2220A requires a tribal government to have a Cybersecurity Plan that meets 13 required statutory elements, as determined by the CISA Director, to receive a grant under TCGP. The Cybersecurity Plan Template is provided as an optional tool for eligible Tribal governments to use to develop and submit their cybersecurity plans with their grant applications to help ensure their plans meet the 13 required statutory elements. Ultimately, Tribal governments are encouraged to develop a plan that reflects their unique situation while meeting program requirements. This includes using existing plans and documents to the extent that any plans of the tribal government protect against cybersecurity risks and cybersecurity threats to information systems owned or operated by or on behalf of the tribal government.

   Cybersecurity Plans are intended to be strategic in nature and do not represent a firm commitment to complete all associated activities in alignment with respective objectives within a given period of performance. Additionally, Cybersecurity Plans are intended to be living documents and a tribal government, following the post-award submission of its final plan, may later update that plan. FEMA and CISA are available to provide technical assistance to Tribal governments on Cybersecurity Plan development. Tribal governments can connect with their FEMA Tribal Liaisons if they need assistance in locating their respective CISA regional Cybersecurity Advisor or Cybersecurity State Coordinator.

While a living document, the Cybersecurity Plan Template must have sufficient information for FEMA/CISA to conduct a meaningful review as part of the TCGP. Eligible recipients must include at least one IJ, one PW, and one completed Cybersecurity Plan or the Cybersecurity Plan Template as part of the overall post-award submission through FEMA GO. If a tribe already has a cybersecurity plan, then the plan should be submitted with the IJ and PW as part of their post-award submission in FEMA GO.

Recipients can email questions about the IJ, PW, Cybersecurity Plan or Cybersecurity Plan Template application requirements to FEMA-TCGP@fema.dhs.gov.

4. SF-424A, Budget Information (Non-Construction)
Standard Forms may be accessed in the Forms tab under the SF-424 family on Grants.gov. For more information, recipients may email at FEMA-TCGP@fema.dhs.gov.

5. SF-424B, Standard Assurances (Non-Construction)
Standard Forms may be accessed in the Forms tab under the SF-424 family on Grants.gov. For more information, recipients may email at FEMA-TCGP@fema.dhs.gov.

12. Appendix C: Required, Encouraged, and Optional Services and Resources

All TCGP recipients are required to participate in a limited number of free services by CISA. Note that participation is not required for submission and approval of a grant but is a post-award requirement. All TCGP recipients are strongly encouraged to participate in other memberships. Additionally, optional CISA resources are also available in this appendix.

Required Services

Cyber Hygiene Services

Vulnerability scanning evaluates external network presence by executing continuous scans of public, static Internet protocols for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts.

To register for this service, email vulnerability@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services – TCGP" to get started. Indicate in the body of your email that you are requesting this service as part of TCGP. For more information, visit CISA's Cyber Hygiene Information Page.

Encouraged Services, Membership and Resources

Cyber Protective Visits

Prior to conducting a formal engagement with a tribe, such as an assessment or workshop, a Cybersecurity Advisor (CSA) may first conduct an initial visit to both gauge the tribe's interest in DHS's cybersecurity offerings and gain a better understanding of its needs and orientation within the broader cybersecurity landscape. Given the important role that these visits play in laying the foundation for future engagement and partnership, CSAs must conduct the preparation necessary to ensure that a favorable first impression is made.

CISA Recommended Resources, Assessments, and Memberships (not mandatory)

The Cyber Resource Hub is a recommended site for Tribal governments that provides a comprehensive list of cybersecurity resources.

In addition to these resources, CISA's Interoperable Communications Technical Assistance Program (ICTAP) provides direct support to tribal emergency responders and government officials across all 56 states and territories through training, tools, and onsite assistance to advance public safety interoperable communications capabilities. These services are provided at no cost and scalable to the community's needs. Within the catalog, the 9-1-1/Public Safety Answering Point/Land Mobile Radio Cyber Assessment technical assistance offering provides organizations with a review of their cyber posture in accordance with nationally recognized best practices guidelines. CISA employs the NIST Special Publication 800-53, Rev 5, "Security and Privacy Controls for Information Systems and Organizations" as a framework. Requests for ICTAP assistance are coordinated through the Statewide Interoperability Coordinator from each state, territory, and tribe.

CISA Central: To report a cybersecurity incident, visit https://www.us-cert.gov/report.

For additional CISA services visit the CISA Services Catalog.

All Resources & Tools | CISA allows users to filter by audience (e.g., State, Local, Tribal, and Territorial Government or Educational Institutions) when browsing available resources.

All membership costs utilizing TCGP funding must be approved in advance by FEMA.

13. Appendix D: Sample Performance Progress Report (PPR) and Sample Cyber Performance Narrative for Progress Reporting

The Sample PPR and Sample Cyber Performance Narrative on the following pages include examples of performance metrics and other data necessary to satisfy TCGP programmatic reporting requirements. Grant recipients are encouraged to use these samples and the instructions therein to prepare and submit annual progress reporting data for TCGP awards.

PERFORMANCE PROGRESS REPORT
SF-PPR

		Page | of Pages
1. Federal Agency and Organization Element to Which Report is Submitted Federal Emergency Management Agency	2. Federal Grant or Other Identifying Number Assigned by Federal Agency EMW-2025-CY-12345	3a. DUNS Number 123456789 3b. EIN 123456789
4. Recipient Organization (Name and complete address including zip code) Roaring River Tribal Community Emergency Management Agency 1234 Happy St. Land, U.S.A. 00000 5.		Recipient Identifying Number or Account Number
6. Project/Grant Period Start Date: (Month, Day, Year) 12/01/2025 End Date: (Month, Day, Year) 11/30/2029	7. Reporting Period End Date (Month, Day, Year) 12/31/2026	8. Final Report? ☐ Yes ☒ No 9. Report Frequency ☑ annual ☐ semi-annual ☐ quarterly ☐ other (If other, describe: _____)

10. Performance Narrative *(attach performance narrative as instructed by the awarding Federal Agency)*

Federal Award Amount - $1,234,567; Cost Share (% provided by recipient here)
Total Federal Funding for Management and Administration (5% M&A) - $61,728.35
Total Federal Funding for Projects - $612,000
Total Federal Funding "To Be Determined" for Projects - $560,838.65
Expended to date and drawdown Federal Funding for Projects Only - $55,249.25
Expended to date and drawdown Federal Funding for M&A Only - $35,000.00
Total Federal Funding Expended to Date: $90,249.25
Remaining Balance of Federal Funding for Projects Only - $556,750.75
Remaining Balance of Federal Funding for M&A - $26,728.35
Remaining Balance of Federal Funding "To Be Determined" for Projects - $560,838.65
Remaining Federal Funding Balance - $1,144,317.75

Statewide Cybersecurity Plan approved by FEMA/CISA. The recipient certifies that all of the grant funding used to support emergency communications investments will comply with the SAFECOM Guidance on Emergency Communications Grants (SAFECOM Guidance). The recipient's conformance with the SAFECOM Guidance ensures that federally funded investments are compatible, interoperable, resilient, and support national goals and objectives for improving emergency communications. See attachment for performance narrative.

11. Other Attachments *(attach other documents as needed or as instructed by the awarding Federal Agency)*

12. Certification: I certify to the best of my knowledge and belief that this report is correct and complete for performance of activities for the purposes set forth in the award documents.

12a. Typed or Printed Name and Title of Authorized Certifying Official Ms. Jane Smith, Director	12c. Telephone *(area code, number and extension)* 1-234-567-890 12d. Email Address roaringriver@ema.gov
12b. Signature of Authorized Certifying Official Jane Smith	12e. Date Report Submitted *(Month, Day, Year)* 1/30/26 13. Agency use only

FY 2025 TCGP Performance Narrative: Roaring River Tribal Community

Narrative of Overall Projects Status

Insert a narrative of the overall project status in this section.

Roaring River Tribal Community Project Expenditures

The Roaring River Tribal Community has 4 CISA-approved projects, obligating $612,000 in Federal funds with $55,249.25 total expenditures to date for approved project funding only. CISA-approved projects include the following:

Project Name as detailed on approved Project Worksheet:	Expenditures to date:
Endpoint Detection Project	*$87,000*
Cybersecurity Training Course for Local Jurisdictions Project	*$300,000*
CISO Firewall Upgrade Project	*$150,000*
Cyber Risk Assessment Project	*$75,000*

Note: Another option for reporting the expenditure-to-date and remaining balance information per project is to add a column to the CISA-approved Project Worksheet and providing that with the PPR submission.

Roaring River Tribal Community Cybersecurity Plan Metrics

Project Objectives	Program Sub-Objectives	Associated Metrics	Metric Description
1. Implement a centralized cybersecurity governance structure, policies, processes and baseline measures to build and maintain cyber resiliency across the state.	*1.1 Develop and institutionalize the state's cybersecurity framework based on the NIST CSF.*	*80%* *Percentage of local government entities which have implemented the cybersecurity framework based on their individual risk profile.*	*The total number of local government entities which have implemented the cybersecurity framework by the total number of local government entities responding to a request for that information.*

Roaring River Tribal Community Performance Measures

Performance metrics vary across the fiscal years and programs (TCGP). Recipients should ensure they are using the **correct** performance measures for their submitted performance narratives. The specific measures can be found in the NOFOs linked below:

- FY 2023 TCGP
- FY 2025 TCGP

The chart below is a *sample* of how a recipient would complete the performance measures using the **FY 2025 TCGP NOFO** requirements for Performance Measures (3E).

Responses for Performance Measures requesting "Percentage of" should either be "100%" for completed status or "0" for incomplete/in progress status. Metrics should be answered on behalf of your TCGP program to CISA as "Entities" equals tribal nation. When the metric value is zero, responses should be entered as "0."

Performance Measure	Quantified Metric
Percentage of tribes with CISA approved tribal Cybersecurity Plans (100% target range – statutorily required)	100%
Percentage of tribes with Tribal Cybersecurity Planning Committees that meet the Homeland Security Act of 2002 and TCGP funding notice requirements (100% target range – statutorily required)	100%
Percentage of tribes conducting annual table-top and full-scope exercises to test Cybersecurity Plans (40% target range)	100%
Percent of the tribes' TCGP budget allocated to exercises (10% target range)	100%
Average dollar amount expended on exercise planning for tribes (10% target range)	0
Percentage of tribes conducting an annual cyber risk assessment to identify cyber risk management gaps and areas for improvement (70% target range)	0
Percentage of tribes performing phishing training (50% target range)	100%
Percentage of tribes conducting awareness campaigns (90% target range)	0
Percent of tribes providing role-based cybersecurity awareness training to employees (60% target range)	100%
Percentage of tribes with capabilities to analyze network traffic and activities related to potential threats (60% target range)	0
Percentage of tribes implementing multi-factor authentication (MFA) for all remote access and privileged accounts (70% target range)	100%
Percentage of tribes with programs to anticipate and discontinue use of end-of-life software and hardware (60% target range)	0
Percentage of tribes prohibiting the use of known/fixed/default passwords and credentials (75% target range)	0
Percentage of tribes operating under the ".gov" internet domain (50% target range)	100%
Number of cybersecurity gaps or issues addressed annually by tribes (50% target range)	100%
Percentage of tribe-created performance metrics that were met (50% target range)	0
Percentage of tribes participating in CISA services (50% target range)	0
Percentage of tribes that have implemented data encryption projects (50% target range)	100%
Percentage of tribes that have implemented enhanced logging projects (60% target range)	0

14. Appendix E: POETE Solution Areas for Investments

Overview
Funding guidelines established within this section support developing, updating, and implementing a Cybersecurity Plan. Allowable investments made in support of this program must fall into the categories of POETE, aligned to closing capability gaps or sustaining capabilities.

Guidance
Section 2220A(n)(6) of the *Homeland Security Act of 2002* (codified as amended at 6 U.S.C. § 665g(n)(6)) prohibits recipients under the TCGP from using a "grant awarded…to construct, remodel, or perform alterations of buildings and other physical facilities." However, this section does not prohibit a recipient from making a minor modification to an existing building or other physical facility necessary to install and connect equipment purchased under a grant award or subaward, such as drilling a hole in a building's wall to mount that equipment. In addition, the prohibition under Section 2220A(n)(6) does not apply in circumstances where a recipient or subrecipient constructs, remodels or performs alterations of buildings or other physical facilities with its own funding when installing and connecting equipment for an information system purchased under a grant award or subaward. The prohibition under Section 2220A(n)(6) only applies to work and associated costs sourced with federal funding and/or the nonfederal share of a grant award and does not apply to work completed at a recipient's or subrecipient's own expense.

Recipients and subrecipients may use TCGP funding to perform minor modifications that **do not** substantially affect a building's, or other physical facility's, structure, layout or systems; affect critical aspects of a building's safety; or otherwise materially increase the value or useful life of the building or other physical facility. The prohibition would also apply to the nonfederal cost-sharing requirement detailed in Section 2220A(m) (codified as amended at 6 U.S.C. § 665g(m)). As a reminder, all projects and associated budgets must support the approved Cybersecurity Plan and be approved in advance by the Cybersecurity and Infrastructure Security Agency and FEMA.

Examples of the types of minor modifications that could be **allowable** with TCGP funding and the non-federal cost share are listed below:

- Fastening equipment to building or other physical facility walls where it does not become a permanent fixture (such as hanging a server rack with servers on a building wall).
- Replacing an outdated existing electrical or internet outlet into which the equipment will connect.
- Installing new cabling.
- Replacing existing cabling.
- Moving cabling.
- Installing and connecting information system equipment to the building's network and power supply and internet.
- Making a hole in the wall to attach the equipment to the building's network, power or internet.

Unallowable remodeling and alterations include permanent modifications that substantially affect the building's, or other physical facility's, structure, layout or systems; affect critical aspects of a building's or other physical facility's safety (such as structural integrity and fire safety systems); or other modifications that materially increase the value or useful life of the building or other physical facility.

Examples of the types of construction, remodeling and alterations that are **unallowable** with TCGP funding, or the non-federal cost share, are listed below:

- Constructing a new building or other physical facility.
- Updating an electrical system to a building or other physical facility that involves work to enhance or modernize the electrical infrastructure, such as replacing electrical panels, upgrading old or unsafe wiring, and replacing circuit breakers.
- Installing new walls or reconfiguring existing walls.
- Affixing equipment in such a way that it becomes a permanent part of a building or other physical facility (as this would result in the equipment no longer being personal property).

Because Section 2220A(n)(6) does not apply to minor modifications that do not: substantially affect a building or other physical facility's structure, layout, or systems; affect critical aspects of a building or other physical facility's safety; or otherwise materially increase the value or useful life of a building or other physical facility, minor modifications **may be permitted under the TCGP subject to additional reviews**. As a reminder, recipients are required to submit projects for minor building modifications approval to the FEMA Grant Programs Directorate Environmental Planning and Historic Preservation Branch. Questions regarding this requirement may be directed to FEMA-TCGP@fema.dhs.gov.

Planning

Planning costs are allowable under this program. TCGP funds may be used for a range of planning activities, such as those associated with the development, review, and revision of the holistic, entity-wide Cybersecurity Plan and other planning activities that support the program goals and objectives and Cybersecurity Planning Committee requirements. **FEMA will not release funds to a recipient until CISA approves the entity's Cybersecurity Plan**. Planning activities may include the following:

- Update or revision of a Cybersecurity Plan;
- Cybersecurity incident response plans or planning; and
- Business continuity and/or disaster recovery plans.

Organization

Organization costs are allowable under this program. Tribal governments must justify proposed expenditures of TCGP funds to support organization activities within their Investment Justifications and Project Worksheet submissions. Organizational activities may include the following:

- Program management;
- Development of whole community partnerships that support the approved Cybersecurity Planning Committee;
- Structures and mechanisms for information sharing between the public and private sector; and

- Operational support.

Personnel hiring, overtime, and backfill expenses are permitted under this grant to perform allowable TCGP POETE activities. Personnel expenses may include, but are not limited to training and exercise coordinators, program managers and planners, and cybersecurity navigators. The grant recipient must demonstrate that the personnel will be sustainable once the program ends or funds are no longer available.

Equipment
Equipment costs are allowable under this program. TCGP equipment is intended to be used to address cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, SLTT governments.

Recipients will be responsible for obtaining and maintaining all necessary certifications and licenses for the requested equipment. Investments in emergency communications systems and equipment must meet applicable SAFECOM Guidance on Emergency Communications Grants recommendations. Such investments must be coordinated with the Statewide Inoperability Coordinator (SWIC) and the State Interoperability Governing Body (SIGB) to ensure interoperability and long-term compatibility.

TCGP funds may be used to purchase maintenance contracts or agreements, warranty coverage, licenses, and user fees in support of a system or equipment. These contracts may exceed the period of performance if they are purchased incidental to the original purchase of the system or equipment, as long as the original purchase of the system or equipment is consistent with that which is typically provided for, or available through, these types of agreements, warranties, or contracts.

When purchasing a stand-alone warranty or extending an existing maintenance contract on a system or an already-owned piece of equipment, coverage purchased may not exceed the period of performance of the award used to purchase the maintenance agreement or warranty, and it may only cover equipment purchased with TCGP funds or for equipment dedicated for TCGP-related purposes. As with warranties and maintenance agreements, this extends to licenses and user fees as well.

The use of TCGP grant funds for maintenance contracts, warranties, repair or replacement costs, upgrades, and user fees are allowable, unless otherwise noted. Except for maintenance plans or extended warranties purchased incidental to the original purchase of the equipment, the period covered by maintenance or warranty plan must not exceed the period of performance of the specific grant funds used to purchase the plan or warranty.

Training
Training costs are allowable under this program. Allowable training-related costs under TCGP include the establishment, support, conduct, and attendance of training or in conjunction with training by other federal agencies. Training conducted using TCGP funds should align to the eligible entity's approved Cybersecurity Plan, address a performance gap identified through assessments, and contribute to building a capability that will be evaluated through a formal exercise. Recipients are encouraged to use existing training rather than developing new courses.

When developing new courses, recipients are encouraged to apply the Analyze, Design, Develop, Implement, and Evaluate model of instructional design.

Recipients are also encouraged to use FEMA's National Preparedness Course Catalog. Trainings include programs or courses developed for and delivered by institutions and organizations funded by FEMA. This includes the Center for Domestic Preparedness, the Emergency Management Institute, and FEMA's Training Partner Programs, including the Continuing Training Grants, the National Domestic Preparedness Consortium, the Rural Domestic Preparedness Consortium, and other partners. The catalog features a wide range of course topics in multiple delivery modes to meet FEMA's mission scope as well as the increasing training needs of federal, state, local, and territorial audiences.

Some training activities require Environmental and Historic Preservation (EHP) Review, including exercises, drills, or **trainings that require any type of land, water, or vegetation disturbance or building of temporary structures or that are not located at facilities designed to conduct training and exercises**. Additional information on training requirements and EHP review can be found online at Environmental Planning and Historic Preservation | FEMA.gov.

CISA's Federal Virtual Training Environment offers cybersecurity training to federal, state, local, tribal, and territorial government employees, which offer education and certifications aligned with the NICE Workforce Framework for Cybersecurity. Additional information can be found at CISA Learning | National Institute for Cybersecurity Careers and Studies.

Exercises

Exercise costs are allowable under this program. Exercises conducted with grant funding should be managed and conducted consistent with the Homeland Security Exercise and Evaluation Program (HSEEP). HSEEP guidance for exercise design, development, conduct, evaluation, and improvement planning is located at HSEEP | FEMA.gov.

Some exercise activities require EHP review, including exercises, drills, or trainings that require any type of land, water, or vegetation disturbance or building of temporary structures or that are not located at facilities designed to conduct training and exercises. Additional information on exercise requirements and EHP review can be found online at Environmental Planning and Historic Preservation | FEMA.gov.

15. Appendix F: Sample Budget Worksheet and Budget Narrative

Sample Budget Detail Worksheet and Narrative

Purpose. The Budget Detail Worksheet and Budget Narrative may be used as a guide to assist applicants in the preparation of the budget and budget narrative. Applicants may submit the budget and budget narrative using this form or in the format of their choosing (plain sheets, independently created forms, or a variation of this form). However, all required information (including the budget narrative) must be provided. Any category of expense not applicable to the applicant's budget may be deleted.

A. Personnel. List each position by title and name of employee, if available. Show the annual salary rate and the percentage of time to be devoted to the project. Compensation paid for employees engaged in grant activities must be consistent with that paid for similar work within the applicant organization.

Name/Position	Computation	Cost
Title:	Hours x rate	$
	Total Personnel	$

B. Fringe Benefits. Fringe benefits should be based on actual known costs or an established formula. Fringe benefits are for the personnel listed in budget category (A) and only for the percentage of time devoted to the project.

Name/Position	Computation	Cost
Title	Hours x rate	$
	Total Fringe Benefits	$

C. Travel. Itemize travel expenses of project personnel by purpose (e.g., staff to training, field interviews, advisory group meeting, etc.). Show the basis of computation (e.g., six people to 3-day training at $X airfare, $X lodging, $X subsistence). In training projects, travel and meals for trainees should be listed separately. Show the number of trainees and unit costs involved. Identify the location of travel, if known. Indicate source of any Travel Policies applied.

Purpose of Travel	Location	Item	Computation	Cost
training	Name of location/address	POV Mileage	Rate x #miles	total
training	same	Applicable flight	Rate x #people	total
		Per diem	Rate x #people	
		hotels	Rate x #nights x #people	
				$
		Total Travel		$

D. Equipment. List non-expendable items that are to be purchased. Non-expendable equipment is tangible property having a useful life of more than one year. (Note: Organization's own capitalization policy and threshold amount for classification of equipment may be used). Expendable items should be included either in the "Supplies" category or in the "Other" category. Applicants should analyze the cost benefits of purchasing versus leasing equipment, especially high cost items and those subject to rapid technical advances. Rented or leased equipment costs should be listed in the "Contractual" category. Explain how the equipment is necessary for the success of the project. Attach a narrative describing the procurement method to be used.

Budget Narrative: Provide a narrative budget justification for each of the budget items identified.

Item	Computation	Cost
Name and how many	Price per unit	Total $
	Total Equipment	$

E. Supplies. List items by type (office supplies, postage, training materials, copying paper, and other expendable items such as books, hand held tape recorders) and show the basis for computation. (Note: Organization's own capitalization policy and threshold amount for classification of supplies may be used). Generally, supplies include any materials that are expendable or consumed during the course of the project.

Supply Items	Computation	Cost
Name and how many	Price per unit	Total $
	Total Supplies	$

F. Consultants/Contracts.

***Consultant Fees*:** For each consultant enter the name, if known, service to be provided, hourly or daily fee (8-hour day), and estimated time on the project. Include any pre-award grant writing services provided by a consultant in this section (maximum cost is $1,500 per applicant)

Budget Narrative: Provide a narrative budget justification for each of the budget items identified.

Name of Consultant	Service Provided	Computation	Cost
			$
		Subtotal – Consultant Fees	$

Consultant Expenses: List all expenses to be paid from the grant to the individual consultant in addition to their fees (i.e., travel, meals, lodging, etc.)

Budget Narrative: Provide a narrative budget justification for each of the budget items identified.

Item	Location	Computation	Cost
			$

Subtotal – Consultant Expenses	$

***Contracts*:** Provide a description of the product or services to be procured by contract and an estimate of the cost. Applicants are encouraged to promote free and open competition in awarding contracts. Any sole source contracts must follow the applicable requirements set forth in 2 C.F.R. §§ 200.317 through 200.326.

Budget Narrative: Provide a narrative budget justification for each of the budget items identified.

Item	Cost
	$
Subtotal – Contracts	$
Total Consultants/Contracts	$

G. Other Costs. List items (e.g., reproduction, janitorial or security services, and investigative or confidential funds) by major type and the basis of the computation. For example, provide the square footage and the cost per square foot for rent, and provide a monthly rental cost and how many months to rent.

Budget Narrative: Provide a narrative budget justification for each of the budget items identified.

Important Note: If applicable to the project, construction costs should be included in this section of the Budget Detail Worksheet.

Description	Computation	Cost
		$
	Total Other	$

H. Indirect Costs. Indirect costs are allowed only if the applicant has a federally approved indirect cost rate. A copy of the rate approval, (a fully executed, negotiated agreement), must be attached. If the applicant does not have an approved rate, one can be requested by contacting the applicant's cognizant Federal agency, which will review all documentation and approve a rate for the applicant organization, or if the applicant's accounting system permits, costs may be allocated in the direct costs categories.

Description	Computation	Cost
		$
	Total Indirect Costs	$

I. Budget Summary. When applicant has completed the budget worksheet, transfer the totals for each category to the spaces below. Compute the total direct costs and the total project costs. Indicate the amount of Federal funds requested and the amount of non-Federal funds that will support the project.

Budget Category	Federal Amount	Non-Federal Amount
A. Personnel	$	$
B. Fringe Benefits	$	$
C. Travel	$	$
D. Equipment	$	$
E. Supplies	$	$
F. Consultants/Contracts	$	$
G. Other	$	$
H. Indirect Costs	$	$

Total Requested Federal Amount	Total Non-Federal Amount
$	$
Combined Total Project Costs	
$	