



# FY 2025 Tribal Cybersecurity Grant Program FAQs



## Contents

|                                                                                                                            |   |
|----------------------------------------------------------------------------------------------------------------------------|---|
| BACKGROUND .....                                                                                                           | 3 |
| GENERAL PROGRAM QUESTIONS .....                                                                                            | 3 |
| What is the purpose of the Tribal Cybersecurity Grant Program (TCGP)? .....                                                | 3 |
| UPDATED: How much funding is available? .....                                                                              | 3 |
| UPDATED: How will funds be allocated? .....                                                                                | 3 |
| UPDATED: Who is eligible to apply? .....                                                                                   | 3 |
| Is the Tribal Cybersecurity Grant Program (TCGP) related to the Tribal Homeland Security Grant Program (THSGP)? .....      | 4 |
| Is the Tribal Cybersecurity Grant Program (TCGP) related to the State and Local Cybersecurity Grant Program (SLCGP)? ..... | 4 |
| When will Tribal governments receive funding? .....                                                                        | 4 |
| UPDATED: What is the goal of the program and its corresponding objectives? .....                                           | 4 |
| UPDATED: What are the required programmatic conditions of receiving a TCGP grant? .....                                    | 4 |
| UPDATED: Are there services that recipients are required to utilize? .....                                                 | 5 |
| When are TCGP key dates? .....                                                                                             | 5 |
| UPDATED: How long is the period of performance (POP)? .....                                                                | 5 |
| UPDATED: How will proposed projects be evaluated? .....                                                                    | 5 |
| Are there any Cybersecurity Plan examples or templates? .....                                                              | 6 |
| NEW: What type of information must be included in the PW and IJs? .....                                                    | 6 |
| COST SHARE .....                                                                                                           | 7 |
| Is there a cost share requirement for the TCGP? .....                                                                      | 7 |
| CYBERSECURITY BEST PRACTICES .....                                                                                         | 7 |
| Are there specific best practices that Tribal governments should adopt? .....                                              | 7 |
| ELIGIBLE EXPENSES .....                                                                                                    | 7 |
| How can the grant funds be used? .....                                                                                     | 7 |
| Can personnel be hired with grant funds? .....                                                                             | 8 |
| What equipment or software should be purchased? .....                                                                      | 8 |
| CYBERSECURITY PLANNING COMMITTEE .....                                                                                     | 8 |
| What are the Cybersecurity Planning Committee membership requirements? .....                                               | 8 |
| Can existing committees be used? .....                                                                                     | 8 |
| What are the responsibilities of the planning committee? .....                                                             | 8 |
| What is the Cybersecurity Planning Committee Charter? .....                                                                | 9 |

|                                                                                                    |    |
|----------------------------------------------------------------------------------------------------|----|
| How should planning committees prioritize individual projects? .....                               | 9  |
| CYBERSECURITY PLANS .....                                                                          | 9  |
| Who is required to submit a Cybersecurity Plan? .....                                              | 9  |
| Who must approve the Cybersecurity Plan before it is submitted to DHS? .....                       | 9  |
| Can I revise my Cybersecurity Plan? .....                                                          | 9  |
| Are there specific requirements for the Cybersecurity Plan? .....                                  | 10 |
| Is DHS able to provide technical assistance to help with Cybersecurity Plan revision? .....        | 10 |
| Can funds be used to enhance existing efforts? .....                                               | 10 |
| Can existing plans be used? .....                                                                  | 10 |
| What will DHS do with the Cybersecurity Plan? .....                                                | 10 |
| Is there a template or guidance for the Cybersecurity Plan? .....                                  | 10 |
| PERFORMANCE MEASURES .....                                                                         | 11 |
| NEW: What are the FY 2025 TCGP Performance Measures? .....                                         | 11 |
| ADDITIONAL INFORMATION .....                                                                       | 11 |
| Where can I go for more information? .....                                                         | 11 |
| What other resources are available to address programmatic, technical, and financial questions? .. | 11 |

## BACKGROUND

Tribal nations face unprecedented cybersecurity risks, including increasingly sophisticated adversaries, widespread vulnerabilities in commonly used hardware and software, and broad dependencies on networked technologies for the day-to-day operation of critical infrastructure. Cyber risk management is further complicated by the ability of malicious actors to operate remotely, linkages between cyber and physical systems, and the difficulty of reducing vulnerabilities.

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 the Tribal Cybersecurity Grant Program (TCGP). Through funding from the Infrastructure Investment and Jobs Act (IIJA), 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.

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

## GENERAL PROGRAM QUESTIONS

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

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

### UPDATED: How much funding is available?

The total amount of funds available under the TCGP for FY 2025 is approximately \$12.1 million. This amount combines available funding from FY 2024 and FY 2025. The funding appropriated for the TCGP for FY 2024 is \$9,142,966 and FY 2025 is \$3,021,975 respectively.

### UPDATED: How will funds be allocated?

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. Additional information is available in the FY 2025 TCGP NOFO Section 3. “Program Description”.

### UPDATED: Who is eligible to apply?

The only eligible Tribal applicants are those listed in Section 3 of the FY 2025 Tribal Cybersecurity Grant Program Notice of Funding Opportunity, “FY 2025 TCGP Applicants, Investments and Allocations Chart” and applications are limited to only those investments listed in Section 3. Applicants must be a Tribal government that is eligible for the program. “Tribal government” is defined at Section 2220A(a)(7) of the Homeland Security Act (codified as amended at 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.

Tribal governments that apply must submit their Cybersecurity Plan, Cybersecurity Planning Committee List and Charter, in addition to a separate TCGP Investment Justification (IJ) form for each investment/objective in the “FY 2025 TCGP

Applicants, Investments and Allocations Chart,” a Budget Worksheet and Budget Narrative and a Project Worksheet (PW) form. These requirements must be fulfilled before a Tribal government may receive TCGP award funding.

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

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

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

The TCGP and SLCGP are separate grant programs. Tribal governments can apply directly for TCGP funding, whereas tribes are only eligible for SLCGP funding as subrecipients. Tribal governments applying for funding through SLCGP will have to contact their state or territory’s State Administrative Agency (SAA). Tribes can receive funding as a direct recipient through the TCGP and as a subrecipient through the SLCGP. For more information on the SLCGP, please refer to [State and Local Cybersecurity Grant Program](#).

### When will Tribal governments receive funding?

For the FY 2025 application period, awarded Tribal governments will receive funding when they receive their “Notice of Grant Award” in the FEMA GO system, and any applicable funding hold(s) have been lifted.

### UPDATED: What is the goal of the program and its corresponding objectives?

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

- **Governance and Planning:** Develop and establish appropriate governance structures, by implementing and revising Cybersecurity Plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.
- **Assessment and Evaluation:** Identify areas for improvement in a Tribal government’s cybersecurity posture based on continuous testing, evaluation, and structured assessments.
- **Mitigation:** Implement security protections commensurate with risk (outcomes of Objectives 1 and 2), using the best practices as described in element 5 of the required 13 elements of the cybersecurity plans and those further listed in the NOFO.
- **Workforce Development:** Ensure organization personnel are appropriately trained in cybersecurity, commensurate with their responsibilities as suggested in the National Initiative for Cybersecurity Education.

FY 2025 Tribal applicants are limited to applying for the investment/objective number and federal amount included in Section 3. A detailed overview of the program and goals can be found at [SLCGP and TCGP Goals and Objectives](#).

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

For FY 2025, TCGP applicants should satisfy the following programmatic conditions for receiving grant funding:

- Establish a Cybersecurity Planning Committee and accompanying Charter;
- Implement a Cybersecurity Plan, unless the Tribal government has an existing cybersecurity strategic plan that satisfies the requirements outlined in the NOFO;
- Submit a separate IJ form for each investment and objective listed on the draft PW provided by FEMA; and
- Finalize and submit a PW and Budget Worksheet and Budget Narrative based on the draft PW provided by FEMA.

Tribes that have already received an award do not need to submit another cybersecurity plan if they are applying again. However, they will need to re-upload their cybersecurity plan in [FEMA GO](#). For more information, please refer to Appendix A: TCGP Requirements Matrix and Appendix B: Post-Award Program-specific Required Documents, Forms and Information in the FY 2025 NOFO.

### UPDATED: Are there services that recipients are required to utilize?

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

The post-award required services are:

- CISA Cyber Hygiene Services: Vulnerability Scanning – Evaluates external network presence by executing continuous scans of public, static internet protocol (IPs) for accessible services and vulnerabilities. CyHy vulnerability scanning requires no special access to data but identifies public-facing vulnerabilities which may already be exposed to cyber adversaries. Organizations that enroll in [CISA's Cyber Hygiene \(CyHy\)](#) Services typically reduce their risk and exposure by 40% within the first 12 months; most see improvements in the first 90 days. It is about expanding each TCGP recipient's awareness of their organization's dynamic boundaries. From basic asset awareness to daily alerts on urgent findings, Tribal governments will be in a better place to make risk-informed decisions.

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

### When are TCGP key dates?

- August 1, 2025: NOFO released
- August 1, 2025: Application Start Date
- August 15, 2025: Applications due to in the FEMA GO System

### UPDATED: How long is the period of performance (POP)?

The POP for each grant year will be 48 months. The POP begins when an award is announced. However, unlike FY 2023, DHS will not consider requests for any extensions to the POP.

### UPDATED: How will proposed projects be evaluated?

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 Fiscal Year 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.

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

- A FEMA HQ Preparedness Officer reviewed applications to ensure that the applicant met all eligibility requirements and checked submitted applications for completeness.
- CISA organized an objective review panel and directed them to score IJs in line with the programmatic scoring and selection process outlined in the FY 2023 NOFO. Subject Matter Experts (SME) with cybersecurity, grants management and/or tribal engagement experience served as review panelists.

Reviewers evaluated applications, discuss merits within their panels, and scored IJs based on the criteria outlined in the NOFO.

- FEMA HQ Grants Management Specialists sorted investments based on score from highest to lowest. This list is used to develop funding recommendations from the highest score to the lowest score until available FY 2025 TCGP funding has been exhausted.

The review panel scored individual IJs against the following criteria:

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

In the event of a tie during the IJ recommendation determination process, FEMA and CISA gave priority to the tribal government that submitted the Cybersecurity Plan that more effectively meets program objectives and addresses the 13 required Cybersecurity Plan elements. For Tribal Consortium applications, the population category in which the application was reviewed for funding will be based on the largest populated tribe within the Consortium.

More information about the review process and project evaluation criteria can be found in Section 7 in the NOFO.

### Are there any Cybersecurity Plan examples or templates?

Grants.gov has templates for:

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

These templates can be found on FY 2025 TCGP on [grants.gov](https://www.grants.gov) and on [CISA.gov](https://www.cisa.gov) at the [SLCGP and TCGP Cybersecurity Plan Template](#).

### NEW: What type of information must be included in the PW and IJs?

Both the PW and IJ forms have been updated for FY 2025 TCGP. The Project Implementation Schedule Section (p. 4) of the IJ has been removed. The Project Implementation section on the PW has been expanded to capture the related project milestones as well as budget narrative for each proposed project. Completed IJs and the associated PW are not required at the time of application. Completed IJs and the PW are required to be submitted in FEMA GO after awards are made.

FEMA will provide recipients with a draft PW which includes the investment(s) name and number and associated federal amount(s). **Please note that only the investment(s) and associated IJ funding amount(s) on the draft PW are eligible**



**for project funding with FY 2025 TCGP funding.** 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. For additional information, please refer to Appendix B: Post-Award Program-specific required Documents, Forms and Information in the FY 2025 NOFO.

## COST SHARE

### Is there a cost share requirement for the TCGP?

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.

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. However, DHS is not able to provide additional funds even if it does grant a cost share waiver. 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.

## CYBERSECURITY BEST PRACTICES

### Are there specific best practices that Tribal governments should adopt?

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

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

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

## ELIGIBLE EXPENSES

### How can the grant funds be used?

Eligible Tribal governments can use grant funds for:

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

Funds cannot be used for:

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

### Can personnel be hired with grant funds?

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

### What equipment or software should be purchased?

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

## CYBERSECURITY PLANNING COMMITTEE

### What are the Cybersecurity Planning Committee membership requirements?

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

- The tribal government applicant;
- The 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;
- Grants administrative office; and
- Additional tribal representatives are encouraged but not required.

### Can existing committees be used?

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

### What are the responsibilities of the planning committee?

The responsibilities of the Cybersecurity Planning Committee include:

- Assisting with the development, implementation, and revision of the Cybersecurity Plan;
- Approving the Cybersecurity Plan;
- Assisting with the determination of effective funding priorities;
- Coordinating with other committees and like entities with the goal of maximizing coordination and reducing duplication of effort;
- Creating a cohesive planning network that builds and implements cybersecurity preparedness initiatives, using FEMA and other federal resources, and tribal resources; and
- Ensuring investments support closing capability gaps or sustaining capabilities.



## What is the Cybersecurity Planning Committee Charter?

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

The Cybersecurity Planning Committee Charter must have:

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

For more information on Cybersecurity Committees and Committee Charters, please refer to the [SLCGP and TCGP Cybersecurity Planning Committee, Charter Requirements, and Best Practices](#).

## How should planning committees prioritize individual projects?

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

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

## CYBERSECURITY PLANS

### Who is required to submit a Cybersecurity Plan?

Tribal governments must submit Cybersecurity Plans for review and approval as part of their grant applications in order to receive funding if selected. **Tribes that have already received an award in FY 2023 do not need to submit another cybersecurity plan if they are applying again. However, they will need to re-upload their cybersecurity plan and application in [FEMA GO](#).**

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

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

### Can I revise my Cybersecurity Plan?

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

## Are there specific requirements for the Cybersecurity Plan?

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

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

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

The full list of requirements for the Cybersecurity Plan are available on [CISA.gov](https://www.cisa.gov).

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

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

## Can funds be used to enhance existing efforts?

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

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

## Can existing plans be used?

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

## What will DHS do with the Cybersecurity Plan?

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

## Is there a template or guidance for the Cybersecurity Plan?

Yes. CISA offers a downloadable Cybersecurity Plan Template with the other TCGP application documents. This template may be used by Tribal governments or may be referenced as necessary. The template is located on [grants.gov](https://www.cisa.gov/grants.gov) and <https://www.cisa.gov/cybergrants/tcgp>.

## PERFORMANCE MEASURES

### NEW: What are the FY 2025 TCGP Performance Measures?

CISA remains invested in collecting data to gauge program performance. In FY 2025, performance measures were adjusted to better inform applicants of the information CISA will request through the program duration. Each performance measure now includes a recommended target range to better communicate how CISA will measure the program's performance to applicants. Adjusted performance measures include the following:

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

Similar performance measures to those listed above have previously been included in the FY 2023 NOFO. CISA views the implementation of those best practices as informative in determining TCGP's success.

## ADDITIONAL INFORMATION

### Where can I go for more information?

For more information, please visit [cisa.gov/cybergrants](https://cisa.gov/cybergrants).

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

- For additional support and guidance on cybersecurity, Tribal governments should reach out to their CISA Regional Staff. For contact information for each region, please visit [cisa.gov/about/regions](https://cisa.gov/about/regions) or via e-mail at: [TCGPinfo@mail.cisa.dhs.gov](mailto:TCGPinfo@mail.cisa.dhs.gov).

- For additional technical assistance, applicants may contact DHS/FEMA via e-mail at: [FEMA-TCGP@fema.dhs.gov](mailto:FEMA-TCGP@fema.dhs.gov).