CYBERSECURITY GRANT PROGRAM
TRIBAL NATION CONSULTATION

Agenda

- Introduction
- Supporting Tribal Nations
- Summary of the Law and Funding for the Tribal Cybersecurity Grant Program
- FEMA and CISA Roles and Responsibilities
- Program Goal and Objectives
- Planning Committees
- Cybersecurity Plan
- Notional Timeline and Process Overview
- Additional Discussion

Supporting Tribal Nations

- Supporting tribal nations is critical to our national cybersecurity posture. Tribal communities are diverse with unique cultures, histories, political viewpoints, and technical requirements. CISA's goal is to support tribes in securing critical infrastructure.
- CISA, understands that tribal governments have unique challenges when defending against cyber threats like ransomware.
- The State and Local Cybersecurity Improvement Act requires that 3% of appropriated funding be awarded directly to tribal governments and that CISA and FEMA work with Tribal Nations to determine how best to allocate those funds. CISA and FEMA plan for that 3% of funding to be released to tribal governments in its entirety via the Tribal Cybersecurity Grant Program.

Summary of Law – Funding Breakdown

- Eligible entities – States, territories, Tribal Governments (25 USC 5131) and Multi-entity groups of eligible entities
- $1B over 4 years
  - Funds apportioned to FEMA for grants management; CISA identified as subject-matter expert
  - 3% of funds apportioned for Tribal governments
  - Increasing Tribal cost share over time (at the discretion of the DHS Secretary)
- Defined uses of funds (at the discretion of the DHS Secretary)
  - Develop and revise Cybersecurity Plan
  - Implement Cybersecurity Plan
  - Address imminent cybersecurity threats
  - Grant administration (5%)
- The DHS Secretary, in consultation with the Secretary of the Interior and Tribal governments, may prescribe alternative substantively similar requirements for Tribal governments – cybersecurity committee and plan

Annual Funding
- FY22: $200M/$6M
- FY23: $400M/$12M
- FY24: $300M/$9M
- FY25: $100M/3M

Tribal Governments Grant Funding
- 3% Annual Funding

Federal Cost Share
- FY22: 90%
- FY23: 80%
- FY24: 70%
- FY25: 60%

FEMA

Summary of Law - Consultations

The DHS Secretary (or designee) “shall consult with State, local, and Tribal representatives with professional experience relating to cybersecurity, including representatives of associations representing State, local, and Tribal governments”.

The consultations will inform and provide guidance for:

- Grant application process;
- Establishing Cybersecurity Plans;
- Information on risk-based formulas and assessments
- The development of guidelines and requirements;
- Sharing of 3% of the apportionment among tribal entities; and
- Future consultations as necessary.

Roles and Responsibilities

- **CISA – Program Management and Subject Matter Expertise**
  - Define the goals/objectives that define the overarching outcomes for the program;
  - Review and approve cybersecurity plans and projects;
  - Establish measures of effectiveness that demonstrate achievement of goals/objectives.

- **FEMA – Grants Administration Subject Matter Expertise**
  - Conduct eligibility reviews, issue and programmatically and financially manage grant awards consistent with all applicable law, regulations, and policies;
  - Place any special award terms and conditions, in coordination with CISA;
  - Monitor and document recipient progress, in coordination with CISA;
  - Utilize existing FEMA grants and financial management systems that are familiar to grant recipients.

Goal and Objectives

GOAL: Assist SLTT governments with managing and reducing systemic cyber risk.

Governance & Planning	**OBJECTIVE 1**: Develop and establish appropriate governance structures, as well as plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.
Assessment & Evaluation	**OBJECTIVE 2**: SLTT agencies understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation and structured assessments.
Mitigation	**OBJECTIVE 3**: Implement security protections commensurate with risk (outcomes of Objectives 1 & 2)
Workforce	**OBJECTIVE 4**: Ensure organization personnel is appropriately trained in cybersecurity, commensurate with responsibility.

Planning Committee

- Is the structure as described below feasible, or is there a better way to tailor this for tribal needs?
  - Eligible entities shall establish a Cybersecurity Planning Committee
  - Roles
    - Development, implementation, and revision of Cybersecurity Plans
    - Approval of Cybersecurity Plans
    - Assist with determination of effective funding priorities (i.e., individual projects)
  - Required membership
    - Eligible entity
    - Representatives from varying entities
    - Public education
    - Public health
    - 50% of members must have professional experience relating to cybersecurity or information technology

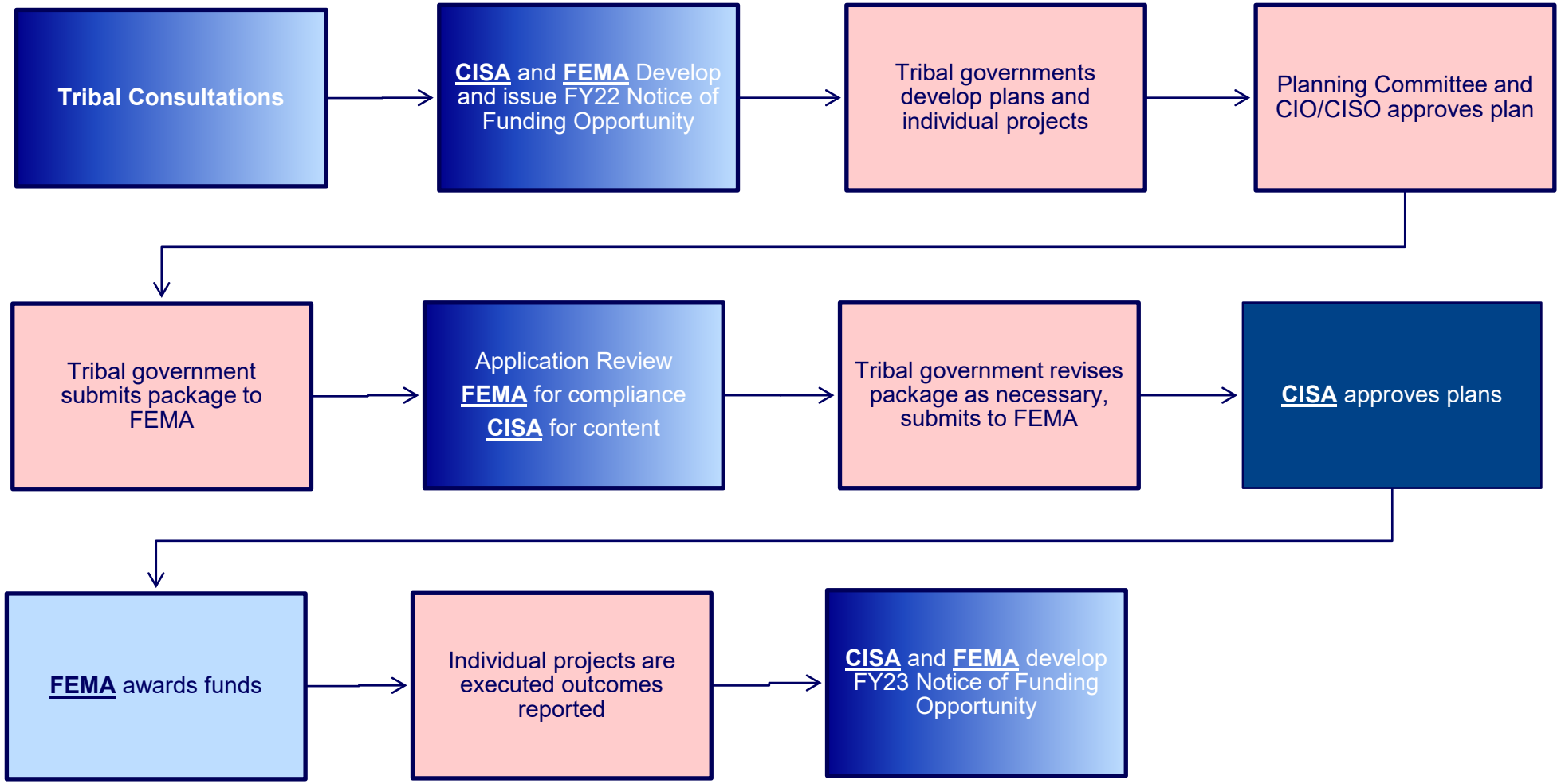
Cybersecurity Plan

- Is the structure as described below feasible, or is there a better way to tailor this for tribal needs?
  - Eligible entities shall submit a Cybersecurity Plan
    - 16 cyber-specific elements
    - Description of the Tribal Governments' roles in overarching plan
    - Assessment of capabilities
    - Resources and timeline for implementing plan
    - Metrics
  - Required Cybersecurity Plans must be approved by Chief Information Officer (CIO) (or equivalent) and planning committee (or equivalent)

Implementation Approach

- Overarching program driven by defined program goal and objectives as described in detail in Appendix A of the NOFO
  - Program Objectives
    - Planning and governance
    - Assessment
    - Mitigation
    - Workforce development
- Cybersecurity Plan is approved by CISA
- The projects will then be approved by CISA and will address the gaps and risks identified by the cybersecurity plan
- Projects will be accomplished over time allowing agencies to use appropriate funding to reduce specific risk

Notional Process Overview



FEMA

Additional Discussion – Q & A