

**U.S. DEPARTMENT OF STATE  
BUREAU OF CYBERSPACE AND DIGITAL POLICY (CDP)  
Notice of Funding Opportunity (NOFO):  
Building International Data Protection and Capacity**

This is the announcement of funding opportunity number DFOP0016688

**Federal Assistance Listing/Catalog of Federal Domestic Assistance Number: 19.665**

**Type of Solicitation:** Open Competition

**Deadline for Applications:** 11:59 PM EST/EDT on 29 July 2024

**Total Funding:** \$1,000,000.00 USD (FY2023)

**Funding Type 1:** Economic Support Funds (ESF)  
**FADR Data Element 2:** Global/Economic Growth/EG8

**Anticipated Number of Awards:** 1

**Type of Award:** Cooperative Agreement

**Period of Performance:** 18 months

**Anticipated Time to Award:** October 2024

**Deadline for Questions:** 11:59 PM EST on 15 July 2024

**Eligibility Category:**

- U.S.- based non-profit/non-governmental organizations subject to sections 501 (c)(3) and 501 (c)(6) of the U.S. tax code
- Private, public, or state institutions of higher education (universities and colleges)
- For-profit organizations or businesses.

**Type of Applicant:** Organizations only. Individuals not eligible to apply.

**Number of Applications:** One (1) per applicant organization.

This notice is subject to availability of funding.

## Section A: Project Description

The U.S. Department of State, Bureau of Cyberspace and Digital Policy (CDP) announces an open competition for organizations with the capacity and interest to carry out the project outlined in this announcement.

Pending the availability of funds, CDP anticipates awarding one grant of up to \$1,000,000.00 USD. CDP reserves the right to award more or less funding or make no award as is in the best interest of the US Government.

This project aims to increase the capacity of partner countries to develop, adopt, and implement legal frameworks that protect individual data privacy while educating key stakeholders and enabling trusted cross-border data flows and digital trade.

The intended target audience of the project activities are data protection agencies and other public institutions with regulatory or enforcement responsibility for data protection and cross-border data flows.

This project will be global.

### A1. Background

Recognizing the growing role of technology as a cross-cutting national security issue, the State Department created the Bureau of Cyberspace and Digital Policy (CDP) in April 2022 to lead and coordinate U.S. diplomacy on cyber and digital policy. The bureau addresses the national security challenges, economic opportunities and human rights considerations presented by cyberspace and digital technologies and promotes standards and norms that are fair, transparent, and support the rights-respecting use of technology. Through robust engagement in multilateral organizations, bilateral diplomacy with partners round the world, and encouragement of responsible state behavior in cyberspace, CDP empowers U.S. leadership in cyber, digital, and technology diplomacy.

CDP deploys foreign assistance to strengthen international cooperation, create new partnerships, promote economic growth and development, and assist in the defense of our foreign partners to uphold an open, interoperable, secure, and reliable Internet.

Calibrated cyber and digital policies help form the backbone of our deeply interconnected world, are vital to U.S. national and economic security, and are required to fully harness the transformative power of technology. As citizens around the world eagerly seek increased Internet connectivity to access the tremendous opportunities afforded by digital transformation, the United States is working to ensure this connectivity is secure, meaningful, governed fairly, and serves the interests of its users. Foreign assistance programs aim to advance an affirmative vision of technology as a tool that supports collective security, prosperity, and democratic values.

More information on CDP is available at <https://www.state.gov/bureaus-offices/deputy-secretary-of-state/bureau-of-cyberspace-and-digital-policy/>.

The Digital Connectivity and Cybersecurity Partnership (DCCP) is a global, interagency initiative led by CDP and the U.S. Department of State to promote an open, interoperable, secure, and reliable internet. DCCP provides foreign assistance to partner nations to promote investments in secure, diverse, and resilient information and communication technologies (ICT) infrastructure; support the adoption of inclusive, rights-respecting, multi-stakeholder models of internet governance, to include data privacy; grow global markets for trusted ICT goods and services, to include cross border dataflow; and enhance cybersecurity. CDP foreign assistance programming follows these core tenets of DCCP. More information on DCCP is available at <https://www.state.gov/digital-connectivity-and-cybersecurity-partnership/>.

As more governments move to adopt data protection laws, we are at critical juncture to build capacity in individual country data protection authorities (DPAs), which have a substantial influence in determining how and when cross-border data flows are legally permissible, and thus the flow of data itself and the underpinning of the global digital economy. Rulemaking and regulatory decisions by DPAs can have significant implications for U.S. firms operating in overseas markets, including firms providing e-commerce and digital services and micro, small, and medium sized enterprises (MSMEs) having limited capacity to react to unpredictable business climates.

A global project is needed to work in partnership with CDP to provide DPAs, and other public institutions with regulatory or enforcement responsibility for data privacy and cross-border data flows, with legislative and regulatory information, training, and capacity building; to expand cooperation with likeminded partners; and to ensure interoperability of frameworks that allow for trusted cross-border data flows. Without amplifying U.S. leadership, potential partners governments may adopt data protection policies that may not appropriately protect individual privacy or preserve the trusted free flow of data needed for an open Internet.

Multiple governments are either in the process of considering comprehensive privacy or data protection legislation or have recently passed related laws and are preparing to establish new data protection authorities or implementing regulations. Failure to support data protection development through holistic training and capacity building could lead to the erosion of U.S. policy leadership as other governments are actively engaging third countries and providing capacity building aligned to contrary policy goals.

Implementer will select beneficiaries for project activities in consultation and coordination with the State Department, via CDP, considering regional and bilateral policy priorities and capacity building needs. In-person events outside the United States shall be coordinated with the local U.S. Embassy officials, via CDP. Regionally focused in-person events may address more than one objective in more than one partner country.

## A2. Strategic Program Goals and Objectives

This project should contribute to the following three CDP strategic goals and objectives outlined in the functional bureau strategy, and three DCCP Pillars.

### **CDP Strategic Goals and Objectives:**

**Bureau Goal 1:** Advance cyber and digital policies that align with U.S. national interests and foreign policy objectives.

- **Objective 1.1:** Deepen relationships with existing U.S. allies and partners, forge new partnerships, and engage with a range of countries to advance a common vision for the Internet and digital technologies.
- **Objective 1.2:** Leverage key multilateral fora to build relationships, advance U.S. policy priorities, and guard against positions that are counter to U.S. approaches to the Internet and digital technologies.
- **Objective 1.3:** Identify, enhance, cultivate, and develop strategic engagements across the private sector and multistakeholder communities.

### **DCCP Pillars:**

**Pillar 1: Build Connections** by promoting investments in secure, diverse, and resilient ICT infrastructure.

**Pillar 2: Advance an Open, Interoperable, Reliable, and Secure Internet** by promoting inclusive, rights-respecting, multi-stakeholder models of internet governance and pro-competition, pro-innovation digital economy policies and regulations.

**Pillar 4: Enhance Cybersecurity** by increasing adoption and implementation of cybersecurity best practices.

## A3. Project Goals, Objectives, Expected Outcomes, Activities, Indicators, and Sustainability

The section below identifies the project goals and objective and details how the project will achieve its objectives through activities designed to achieve specific outcomes in accordance with overarching program (CDP and DCCP) strategic goals and objectives. In awarding funds for this project, CDP expects that the activities and milestones listed below will be accomplished within the project's period of performance.

This project should be designed to achieve the following high-level goal: **Increase the capacity of partner countries to develop, adopt, and implement legal frameworks that protect individual data privacy while educating key stakeholders and enabling trusted cross-border data flows and digital trade.**

**Project Objective 1:** Assist partner countries in developing privacy and data protection laws through workshops, training, and technical assistance to enable DPAs and other agencies regulating data flows to facilitate legal international data transfers with the broad array of mechanisms that currently exist within the partner country.

### **Expected Outcomes**

Achievement of Project Objective 1 is expected to result in the following outcomes:

- Selected partner countries develop and/or adopt new or updated laws and regulations that both preserve individual privacy and enable trusted cross-border data flows.
- Selected partner countries develop and/or adopt new or updated laws, regulations, and/or administrative procedures documenting privacy safeguards related to law enforcement and national security access to data held by private sector entities. Measures may reference OECD Declaration on Government Access to Personal Data Held by Private Sector Entities.

### **Activities**

To achieve the expected project outcomes, the project **must** include the following:

- Analyze proposed legislation and other legal measures, including English translation when not available, in collaboration with CDP and U.S. Embassies.
- Recommend legislative and other policy text based on best practices to facilitate legal data transfers with the broad array of mechanisms that currently exist (adequacy, standard/model contractual clauses, binding corporate rules, certifications and codes of conduct). Coordinate policy recommendations and references with CDP and other U.S. government stakeholders including the Department of Commerce and USTR.
- Recommendations should draw on multilateral, interoperable, enforceable best practices highlighted by CDP, including those documented by multilateral bodies, such as the Global Cross-Border Privacy Rules (CBPR) Forum and the Organization for Economic Cooperation and Development (OECD).
- DPAs and other agencies regulating data flows are able to facilitate legal international data transfers with the broad array of mechanisms that currently exist (adequacy, standard/model contractual clauses, binding corporate rules, certifications and codes of conduct).
- Execute bilateral and/or regional in-person workshops, consultations, or roundtables with government and legislative officials developing or considering legal measures affecting privacy, data protection, and cross-border data flows, including multi-stakeholder formats as necessary.
- Collaborate with the State Department, via CDP, to identify global participants for aforementioned workshops and consultations that include diverse stakeholders currently involved in the development of privacy, data protection, and data flow policies, including technical experts from the private sector, academia, policy makers, third-country officials, and civil society organizations.
- Fund participants and subject matter experts to travel and attend international workshops and other aforementioned engagements, in coordination with the State Department, via CDP.

To achieve the expected project outcomes, the project **could** include the following:

- Comparative analysis of recent and proposed legal measures in select countries and regions, including commonality or reference to multilateral, regional, and/or third-country rules.
- Provide virtual or in-person training to legislative, government, and regulatory officials related to legal, operational, and/or technical matters related to data protection.

**Performance Indicators:**

In addition to project-specific indicators to monitor key milestones and progress to keep the project on track, implementers will report against relevant indicators within the performance management plan CDP established under the auspices of the Digital Connectivity and Cybersecurity Program (DCCP). DCCP indicators for this project will include:

- DCCP 1.8 Number of USG-supported fora held to convene key stakeholders for technical assistance or to discuss digital issues or best practices.
- DCCP 2.1 Number of instances of U.S. ICT/digital policy positions presented in international or regional fora by the U.S. or partner countries.
- DCCP 2.2 Number of ICT/digital governance policies, laws, or regulations drafted, proposed, adopted, improved, or implemented with USG assistance.
- DCCP 2.6 Number of people receiving USG assistance to participate in multilateral fora.
- DCCP 4.11 Number of organizations using or applying principles from internationally recognized frameworks, models, or principles of Internet governance or privacy standards due to USG assistance.

Upon final award, CDP and the selected partner will meet to discuss a final set of DCCP standard indicators as well as project-specific indicators.

**Project Objective 2:** Build capacity of partner countries on the process of establishing data protection authorities through amplification, training, technical assistance, and workshops. Capacity building should include, but not be limited to, facilitating international data transfers drawing on best practices identified by CDP.

**Expected Outcomes**

Achievement of Project Objective 2 is expected to result in the following outcomes:

- Partner countries establish, or take steps towards establishing, data protection authorities.
- Partner country data protection authorities or other regulatory bodies enable interoperable trusted data flows, including through issuing

regulations incorporating mutual recognition, contractual clauses, and/or by issuing appropriate adequacy determinations.

- Partner country data protection authorities adopt open, transparent, consultative, standardized processes in the promulgation of regulations or policy guidance.

### **Activities**

To achieve the expected project outcomes, the project **must** include the following:

- Execute bilateral and/or regional in-person workshops, roundtables, consultations, or training sessions with officials at data protection authorities and other government agencies regulating privacy and data flows, prioritizing those in the process of establishing DPAs. Content could include technical and operational functions of a DPA, including on rulemaking, public consultation, and enforcement, in consultation with the State Department and other U.S. government stakeholders, via CDP.
- Recommend regulatory text based on best practices to facilitate legal data transfers with the broad array of mechanisms that currently exist (adequacy, standard/model contractual clauses, binding corporate rules, certifications and codes of conduct). Coordinate policy recommendations and references with CDP and other U.S. government stakeholders including Commerce and the Federal Trade Commission.
- For countries with greater assistance needs, provide technical assistance to data protection authorities on developing standard operating procedures and internal training curricula, including but not limited to managing public comment processes, use of model/standard contractual clauses, and other administrative processes and technologies related to data protection and international data transfers.
- Collaborate with the State Department, via CDP, to identify global participants for aforementioned workshops and consultations that include diverse stakeholders currently involved in the development of privacy, data protection, and data flow policies, including technical experts from the private sector, academia, policy makers, third-country officials, and civil society organizations.
- Funding participants and subject matter experts to travel and attend international workshops and training, in coordination with the State Department, via CDP.
- Execute virtual seminars for officials at data protection authorities and other government agencies regulating privacy and data flows with subject-matter experts.

To achieve the expected project outcomes, the project **could** include the following:

- Comparative analysis of recent and proposed regulatory measures in select countries and regions, including commonality or reference to multilateral, regional, and/or third-country rules.

- Provide virtual or in-person training to legislative, government, and regulatory officials related to legal, operational, and/or technical matters related to data protection.
- Execute train-the-trainer sessions for data protection authorities' internal personnel and outreach to outside stakeholders, such as major data controllers/processors.

**Performance Indicators:**

In addition to project-specific indicators to monitor key milestones and progress to keep the project on track, implementers will report against relevant indicators within the performance management plan CDP established under the auspices of the Digital Connectivity and Cybersecurity Program (DCCP). DCCP indicators for this project will include:

- DCCP 1.6 Number of people trained in telecom/ICT, digital, or cyber issues with USG support.
- DCCP 1.7 Number of people trained on telecom/ICT or digital issues who demonstrate improved knowledge or skill.
- DCCP 1.8 Number of USG supported fora held to convene key stakeholders for technical assistance or to discuss telecom/ICT or digital issues or best practices.
- DCCP 2.1 Number of instances of U.S. telecom/ICT/digital policy positions presented in international or regional fora by the U.S. or partner countries.
- DCCP 2.2 Number of telecom/ICT governance policies, laws, or regulations drafted, proposed, adopted, improved, or implemented with USG assistance.
- DCCP 2.4 Number of private sector, civil society, or other non-governmental organizations with improved capacity for advocacy or engagement with national legislatures on national telecom/ICT, Internet, or digital policies.
- DCCP 2.6 Number of people receiving USG assistance to participate in multilateral fora.
- DCCP 4.11 Number of organizations using or applying principles from internationally recognized frameworks, models, or principles of Internet governance or privacy standards due to USG assistance.

Upon final award, CDP and the selected partner will meet to discuss a final set of DCCP standard indicators as well as project-specific indicators.

**Project Objective 3:** Build capacity at established data protection authorities in partner countries to collaborate in multilateral efforts promoting trusted cross-border data flows, through training, technical assistance, and workshops. Capacity building should include, but not be limited to, facilitating international data transfers drawing on best practices identified by CDP.

## Expected Outcomes

Achievement of Project Objective 3 is expected to result in the following outcomes:

- Partner countries join, or take steps to join, relevant multilateral organizations, such as but not limited to the Global CBPR Forum and Global Cooperation Arrangement for Privacy Enforcement (Global CAPE).
- Partner countries endorse multilateral principles promoting trusted cross-border data flows, including but not limited to OECD Declaration on Government Access to Personal Data Held by Private Sector Entities and Data Free Flow with Trust.

## Activities

To achieve the expected project outcomes, the project **must** include the following:

- Execute bilateral and/or regional in-person workshops, roundtables, consultations, or training sessions with officials at data protection authorities and other government agencies regulating privacy and data flows. Include multi-stakeholder formats as necessary, including but not limited to networks of DPAs, industry associations, and not-for-profit and civil society privacy experts.
  - Content may include international best practices on interoperable trusted data flows, including mutual recognition, contractual clauses, and/or national adequacy determinations; privacy enhancing technologies (PETS) and other technology factors affecting data protection policy; and management of public comment processes, in consultation with the State Department and other U.S. government stakeholders, via CDP.
- Collaborate with the State Department, via CDP, to identify global participants for aforementioned workshops that include diverse stakeholders currently involved in the development of privacy, data protection, and data flow policies, including technical experts from the private sector, academia, policy makers, the diplomatic community, and civil society organizations.
- Funding participants to travel and attend international workshops and training, in coordination with the State Department, via CDP.
- Execute virtual seminars for officials at data protection authorities and other government agencies regulating privacy and data flows with subject-matter experts.
- Research and brief CDP and other U.S. government officials on engagement and coordination opportunities with foreign DPAs and public institutions with similar roles.

To achieve the expected project outcomes, the project **could** include the following:

- Execute train-the-trainer sessions for data protection authorities' internal personnel and outreach to outside stakeholders, such as major data controllers/processors.
- Advise select partner countries in adopting risk-based data protection measures to mitigate cybersecurity threats and threats from untrustworthy

information and communications technology and services, in coordination with the State Department, via CDP.

**Performance Indicators:**

In addition to project-specific indicators to monitor key milestones and progress to keep the project on track, implementers will report against relevant indicators within the performance management plan CDP established under the auspices of the Digital Connectivity and Cybersecurity Program (DCCP). DCCP indicators for this project will include:

- DCCP 1.6 Number of people trained in telecom/ICT, digital, or cyber issues with USG support.
- DCCP 1.7 Number of people trained on telecom/ICT or digital issues who demonstrate improved knowledge or skill.
- DCCP 1.8 Number of USG supported fora held to convene key stakeholders for technical assistance or to discuss telecom/ICT or digital issues or best practices.
- DCCP 2.1 Number of instances of U.S. telecom/ICT policy positions presented in international or regional fora by the U.S. or partner countries.
- DCCP 2.4 Number of private sector, civil society, or other non-governmental organizations with improved capacity for advocacy or engagement with national legislatures on national telecom/ICT, Internet, or digital policies.
- DCCP 2.6 Number of people receiving USG assistance to participate in multilateral fora.
- DCCP 4.11 Number of organizations using or applying principles from internationally recognized frameworks, models, or principles of Internet governance or privacy standards due to USG assistance.

Upon final award, CDP and the selected partner will meet to discuss a final set of DCCP standard indicators as well as project-specific indicators.

**Sustainability**

Appropriately balancing privacy, economic, security, and human rights equities in data protection laws will ensure they are sustainable without further amendment. Activities building institutional capacity would likewise ensure new laws and regulations are implemented efficiently and in a non-discriminatory manner. Defraying one-time costs associated with drafting legislation, educating key stakeholders, and establishing new institutions will help partner governments facilitate interoperable trusted data flows, which would then have economic and regulatory constituencies to sustain them. Supporting partner government officials in attending regional workshops and Global Cross-border Privacy Forum events would build connections to enable officials from likeminded countries to exchange information and provide mutual support after program concludes. If needed, other U.S. government

departments and agencies may be able to provide out-year assistance to address specialized partner needs not addressed by this program.

#### A4. Key Considerations

The following list of program considerations is provided to help applicant(s) develop a responsive, robust proposal. Strong preference will be given to applicant(s) that:

- Demonstrate administrative and technical capacity and experience in administering successful and similar projects with a global participant base.
- Demonstrate thoughtful project design to address the key objectives and activities for the target audiences described in the NOFO.
- Demonstrate thoughtful monitoring and evaluation and report results.
- Prove existing, collaborative, and successful partnerships with U.S. and foreign partners on issues and engagements related to cybersecurity and digital policy.
- Demonstrate adherence to ethical best practices including “do no harm” and gender equity.

All applicants will also be required to address **the entirety of Section A.3** within this NOFO in their completion of the Draft Scope of Work attached to this NOFO (see Section D.2.1, item #5).

## Section B: Federal Award Information

Organizations may submit one application per organization in response to this NOFO. If more than one application is submitted by an organization, only the first application received will be reviewed for eligibility and funding.

The U.S. government reserves the right to: (a) reject any or all applications, (b) accept other than the lowest cost application, (c) accept more than one application, and (d) waive irregularities in applications received.

The U.S. government may make award(s) based on initial applications received, without discussions or negotiations. Therefore, each initial application should contain the applicant's best terms from a cost and technical standpoint. The U.S. government reserves the right (though it is under no obligation to do so), to enter discussions with one or more applicants in order to obtain clarifications, additional detail, or to suggest refinements in the project description, budget, or other aspects of an application.

CDP anticipates awarding a cooperative agreement. The final determination on award mechanism will be made by the Grants Officer.

The authority for this funding opportunity is found in the Foreign Assistance Act of 1961 (FAA), as amended. Funds were appropriated under the Title III of the Department of State, Foreign Operations and Related Programs Appropriations Act, 2023 (Div. K, P.L. 117-328) (FY 2023

SFOAA) under the heading “Economic Support Funds”. Several funding restrictions apply and may vary from year to year. CDP reserved the right to adjust proposed beneficiaries.

To maximize the impact and sustainability of the award(s) that result(s) from this NOFO, CDP reserves the right to execute a non-competitive continuation amendment(s). The total duration of any award, including potential non-competitive continuation amendments, shall not exceed 54 months, or four and a half years. Any non-competitive continuation is contingent on availability of funds, and satisfactory performance of the program. A non-competitive continuation is not guaranteed, and the Department of State reserves the right to exercise or not exercise this option.

## Section C: Eligibility Information

### C1. Eligible Applicants

CDP welcomes applications from U.S.- based non-profit/non-governmental organizations subject to sections 501 (c)(3) and 501 (c)(6) of the U.S. tax code; Private, public, or state institutions of higher education (universities and colleges); For-profit organizations or businesses.

Please see 2 CFR 200.307 for regulations regarding program income.

### C2. Cost Sharing or Matching

Providing cost sharing, matching, or cost participation **is not** an eligibility factor or requirement for this NOFO and providing cost share will not result in a more favorable competitive ranking. Per 2 CFR §200.306, items that are proposed for cost share must be allowable per 2 CFR §200, Subpart E—Costs Principles.

### C3. Other

To be eligible to receive an award, all organizations must have a unique entity identifier (UEI), as well as a valid registration on [SAM.gov](https://sam.gov). Please see Section D3.2 for information on how to obtain these registrations.

Applicants must be organizations, and only one application will be considered for each applicant organization. If more than one application is submitted by the same organization, only the first received will be reviewed for eligibility and funding.

Applicants must demonstrate existing, or the capacity to develop, active partnerships local in-country partners, entities, and relevant stakeholders and have demonstrable experience in administering successful and preferably similar projects.

Please note, any applicant listed on the Excluded Parties List System in the [System for Award Management \(SAM.gov\)](https://sam.gov) and/or has a current debt to the U.S. government is not eligible to apply for an assistance award in accordance with the OMB guidelines at 2 CFR 180 that

implement Executive Orders 12549 (3 CFR,1986 Comp., p. 189) and 12689 (3 CFR,1989 Comp., p. 235), “Debarment and Suspension.” Additionally, no entity or person listed on the Excluded Parties List System in SAM.gov can participate in any activities under an award. All applicants are strongly encouraged to review the Excluded Parties List System in SAM.gov to ensure that no ineligible entity or person is included in their application.

## Section D: Application and Submission Information

### D1. Address to Request Application Package

Application forms, and other required materials are available at Grants.gov (<http://www.grants.gov>) and MyGrants (<https://mygrants.servicenowservices.com>) under the announcement title “**Building International Data Protection and Capacity**,” and funding opportunity number “DFOP0016688”. Once the NOFO deadline has passed, the Department of State may not discuss this competition with any applicant until the proposal review process has been completed. If requesting reasonable accommodations for persons with disabilities or for security reasons, please contact the CDP point of contact listed in Section G. Please note that reasonable accommodations do not include deadline extensions.

### D2. Content and Form of Application Submission

For all application documents, please ensure:

- The proposal clearly addresses the goals and objectives of this funding opportunity
- All documents are in English (*original documents that are in another language must be accompanied by an English translation*)
- All budgets are in U.S. dollars
- For documents subject to page limitations, all pages are numbered
- All documents are formatted to 8 ½ x 11 paper and,
- All Microsoft Word documents are single-spaced, 12-point Calibri font, with a minimum of 1-inch margins
- Captions and footnotes may be 10-point Calibri font

Any prospective applicant who has questions concerning the contents of this NOFO should submit them by email to the contacts listed in Section G. Any updates about this NOFO will also be posted on [Grants.gov](http://www.grants.gov).

#### D2.1 Application Requirements

Complete applications must include the following:

1. Completed and signed **SF-424**, **SF-424A**, as well as **SF-424B**, if applicable.
2. Organizations that engage in lobbying the U.S. government, including Congress, or pay for another entity to lobby on their behalf, are also required to complete the **SF-LLL** “Disclosure of Lobbying Activities” form.

3. **Cover Page and Executive Summary** (not to exceed three [3] pages, preferably as a Word Document). Includes the organization name, project title, target country or countries, and name and contact information for the application's main point of contact and brief section that clearly outlines the (1) the problem statement addressed by the project (2) research-based evidence justifying the applicant's approach, and (3) quantifiable project outcomes and impacts.
4. **Proposal Narrative** (not to exceed seven [7] pages, preferably as a Word Document). Please note the seven-page limit does not include the following:
  - SF-forms listed above
  - Cover Page and Executive Summary
  - Scope of Work
  - Project Design and Logic Model
  - Project Performance Monitoring and Evaluation Plan
  - Detailed Budget
  - Budget Narrative – *If the Budget includes subawards, please include a separate Budget Narrative for each organization.*
  - Timeline
  - Key Personnel Summary, CVs or Resumes (per person)
  - Contingency Plan
  - Additional Required Attachments (Audit, NICRA, etc.)
  - Optional Sections (*if applicable, see page 15*)

The Proposal Narrative must include the following:

- **Introduction to the Organization:** Description of past and present operations, showing ability to carry out the project, including information on all relevant or similar type projects from previous grants from the Bureau and/or U.S. government agencies.
- **Problem Statement:** Clear, concise, and well-supported statement that summarizes the problem and how the applicant's unique project/approach will address it and support CDP's Strategic Goals and Objectives.
- **Project Goal:** The goal describes the larger outcomes intended.
- **Statement of Capabilities and Experience:** Clear, concise, and well-supported statement that fully describes the applicant's unique project/approach will address both objectives and support CDP's Strategic Goals and Objectives. Applicant should describe past experience with Federal contracting and logistics management, industry knowledge and contacts.
- **Future Funding or Sustainability:** Applicant's plan for continuing the project beyond the grant period, or the availability of other resources, if applicable. Include ways project activities will ensure sustainability.
- **Risk Analysis:** Internal and external risks associated with the proposed project, rate the likelihood of the risks, rate the potential impact of the risks on the project, and identify actions that could help mitigate the risks.

Please note the seven-page limit does not include the following:

- SF-forms listed above
  - Cover Page and Executive Summary
  - Scope of Work
  - Project Design and Logic Model
  - Project Performance Monitoring and Evaluation Plan
  - Detailed Budget
  - Budget Narrative – *If the Budget includes subawards, please include a separate Budget Narrative for each organization.*
  - Timeline
  - Key Personnel Summary, CVs or Resumes (per person)
  - Contingency Plan
  - Additional Required Attachments (Audit, NICRA, etc.)
  - Optional Sections (*if applicable, see page 15*)
5. **Scope of Work (SOW).** Applicants should use the *Project Draft Scope of Work Template (see tab 1)* provided and attached to this NOFO. The SOW should provide a summary of the applicant's unique approach to the following as indicated in Section 4) **Proposal Narrative:**
- **Project Goal**
  - **Project Objectives**
  - **Project Activities**
  - **Project Indicators:** Applicants should also identify key indicators and milestones to measure progress towards program goals and project objectives. Methods for collecting and monitoring project indicators should be described and those responsible for doing so identified.
  - **Sustainability**
6. **Project Logic Model** (preferably as a Word Document). Building out a logic model with an accompanying theory of change can be helpful when planning and designing a program, project or activity. These tools can be used to visually depict or outline how and why a project will work—i.e., the rationale behind your project approach. Detailing how a project's planned activities lead to certain outcomes can often help applicants understand the assumptions within the approach. Detailing factors outside your control, such as policy shifts, within a logic model can identify areas that should be included within your project's risk analysis. It details planned activities, the immediate services or product of project activities (outputs), and the expected changes or benefits that occur after activities have been implemented (outcomes). Applicants should specify objectives, identify what resources (inputs) are needed, outline proposed activities (outputs) and beneficiaries, and illustrate how activities lead to desired results in the theory of change. Applicants are encouraged to use the attached *Project Logic Model Template (see Tab 2)* but are welcome to use their own templates so long as they provide the requisite information for thorough review of the proposed project.

7. **Draft Project Performance Monitoring and Evaluation Plan** (preferably as a Word Document). This document details how a project's performance monitoring and evaluation system will be carried out and by whom. It:
  - Explains how the project's performance toward its objectives will be tracked over time.
  - Identifies which performance indicators the project will report against, the indicator type, baseline values, performance targets, and data sources or collection methods.
  - Provides a clear description of the approach and data collection strategies and tools to be employed (e.g., pre- and post-test surveys, interviews, focus groups).
  - Identifies what, if any, external evaluations will be conducted.

A sample *Project Performance Monitoring and Evaluation Plan Template* (see tab 3) is provided as an attachment to this NOFO. Applicants are encouraged to refer to the *Defining M&E Terms* in the Project Logic Model template for concise explanations of M&E terms and definitions used by the Department of State. **The final will be due 30-60 days post award.**

8. **Project Detailed Budget** (Excel workbook strongly preferred; please **do not** provide as a PDF). Include three (3) columns containing the request to CDP, any cost sharing contribution, and the total budget. A Summary Budget should also be included using the OMB-approved budget categories (see SF-424A as a sample) in a separate tab. Costs must be in U.S. Dollars. Detailed line-item budgets for sub-grantees should be included as additional tabs within the Excel workbook (if available at the time of submission). Please see the attached *Project Detailed Budget Template* (see tab 4) for more information.
9. **Project Budget Narrative** (preferably as a Word Document). Justify each line-item in the budget and explain how the amounts were derived, consistency with the applicants' documented policies, as well as the source and description of all proposed costs (and cost-share, if applicable). The narrative should complement the budget rather than repeat information provided in the budget. For example, the narrative should provide details on the purpose of costs, reasonability of costs, cost price analysis, explain allocations, explain any yearly variances, and tie expenses to project activities and/or objectives where appropriate. Sources of all cost-share offered in the application should be identified and explained in the budget narrative. *Project Budget Narrative Template* (see tab 5) for more information.
10. **Timeline** (not to exceed one [1] page per year of proposed performance period, preferably as a Word Document or Excel Sheet). The timeline of the overall proposal should include activities, and monitoring and evaluation efforts outlined in either a monthly or quarterly format. It should also include sufficient time for project closeout to

conduct and finalize internal/external evaluations and allow any sub-recipients time for final reporting.

11. **Summary of Key Personnel and Subject Matter Experts** (not to exceed two [2] pages, preferably as a Word Document). This can represent staff within your organization or outside of your organization (subgrantee, consultants, contractors), who are integral to the success of the project. Provides names, titles, roles, and bios that highlight relevant experience/qualifications of key personnel involved in the project.
  
12. **Contingency Plan** (not to exceed three (3) pages) for proposed activities should the originally planned activities not be able to be implemented. Applicants should demonstrate consideration of the risks identified in the submitted risk assessment and include specific alternative activities or locations as part of the Contingency Plan. Any proposed “plan” must comply with 2CFR200.433 – Contingency provisions. Plans must not include un-allocable or unallowable expenses and must not result in a larger Total Award Value than the identified as the “competition ceiling.” CDP/SPC requires prior approval by the Grants Officer of the “plan” before any activities can take place, or costs can be incurred against the “plan.”
  
13. **Additional Required Attachments:**
  - **Audit** An audit or an explanation for the lack of an audit is required. Please review the bulleted items below carefully.
    - If your organization meets the threshold as defined in 2 CFR 200 Subpart F, then your organization must submit a pdf of its most recent single audit.
    - If your organization does not currently meet the 2 CFR 200 requirement and has not had a single audit within its most recent three fiscal years, then your organization must submit its most recent (within the preceding three fiscal years) independent financial audit, preferably a pdf.
    - If your organization has not been independently audited within its three most recent fiscal years, then it must explain the reason for the lack of an audit and provide an independent confirmation of the adequacy of its internal controls.
  - **NICRA** If your organization has a Negotiated Indirect Cost Rate Agreement (NICRA) and includes NICRA charges in the budget, your latest NICRA letter should be included as a PDF file. This document will not be reviewed by the Merit Review Panel but will be used by project and grant team if the submission is recommended for funding. Organizations that have previously established indirect cost rates must submit timely indirect cost proposals to their cognizant agency as required by Appendix III & IV of 2 CFR 200. If indirect cost proposals have not been submitted for re-negotiation, as required, out-of-date NICRAs may not be considered. If your proposal involves subawards to organizations charging indirect costs, please submit their NICRA, if applicable.

- Letters of support or official permission letters from project partners describing the roles and responsibilities of each partner, for any partner or partners identified in the proposal whose role is central to the project achieving its objectives. No letter of support is required for goods or services that are widely available commercially unless an identified provider is offering no-cost or uniquely favorable terms that will not be available commercially.

**Applications that do not include the elements listed above will be deemed technically ineligible. To ensure that all applications receive a balanced evaluation, the review panel will review from the first page of each section up to the page limit and no further.**

- **Gender and Inclusion Analysis** (not to exceed two (2) pages, preferably as a Word Document) that provides a concise analysis of relevant gender norms, equity and equality for underserved communities and marginalized populations, power relations, and conflict dynamics in target countries. Potential domains of analysis include institutional practices and barriers, cultural norms, gender roles, access to and control over assets and resources, and patterns of decision-making. Applicants should briefly explain how they have integrated findings from their analysis into project design and/or other proposal documents, including a plan for regularly reviewing and updating the gender and inclusion analysis with local partners/beneficiaries, and making any necessary adjustments to project implementation.

#### D.2.2 Additional Information Requested for Those Receiving Conditional Notification Letter

Successful applicants must submit, after Conditional Notification Letter, but prior to issuance of a federal award:

- Written responses and revised application documents addressing conditions and recommendations from the review panel.
- A copy of the applicant's latest NICRA as a PDF file, if the applicant has a NICRA and includes NICRA charges in the budget.
- A completed copy of the Department's Financial Management Survey, if receiving USG funding for the first time.
- Submission of required documents to register in the Payment Management System managed by the Department of Health and Human Services, if receiving CDP funding for the first time (unless an exemption is provided).
- Other requested information or documents included in the Conditional Notification Letter or subsequent communications prior to issuance of a federal award.
- Applicants who submit their applications through Grants.gov will be required to create a MyGrants account in order to accept the final award. Accounts must be logged into to every 60 days in order to maintain an active account.

### D3. Unique Entity Identifier (UEI) and System for Award Management (SAM)

All organizations, whether based in the United States or in another country, must have a Unique Entity Identifier (UEI) and an active registration with SAM.gov. A UEI is one of the data elements mandated by Public Law 109-282, the Federal Funding Accountability and Transparency Act (FFATA), for all federal awards.

The 2 CFR 200 requires that sub-grantees obtain a UEI number. Please note the UEI for sub-grantees is not required at the time of application but will be required before an award is processed and/or directed to a sub-grantee.

***Note: The process of obtaining or renewing a SAM.gov registration may take anywhere from 4-8 weeks. Please begin your registration as early as possible and advise proposed sub-grantees to do so as well.***

- Organizations **based in the United States** or that pay employees within the United States will need an Employer Identification Number (EIN) from the Internal Revenue Service (IRS) and a UEI number issued through SAM.gov. Once the UEI number is received continue with the remainder of the SAM.gov registration.
- Organizations **based outside of the United States** that do not pay employees within the United States do not need an EIN from the IRS but do need a UEI number – obtained by registering as an entity in SAM.gov.

**Organizations based outside of the United States and that DO NOT plan to do business with the DoD should follow the below instructions:**

Step 1: Proceed to SAM.gov to obtain a UEI and complete the SAM.gov registration process. SAM.gov registration must be renewed annually.

All prime organizations must also continue to maintain active SAM.gov registration with current information at all times during which they have an active federal award or application under consideration by a federal award agency. SAM.gov requires all entities to renew their registration once a year in order to maintain an active registration status in SAM. It is the responsibility of the applicant to ensure it has an active registration in SAM.gov and to maintain that active registration. If an applicant has not fully complied with the requirements at the time of application, the applicant may be deemed technically ineligible to receive an award and use that determination as a basis for making an award to another applicant.

**Note: SAM.gov is not the same as MyGrants. It is free to register in both systems, but the registration processes are different.**

***Information is included on the SAM.gov website to help international registrations:***

[https://www.fsd.gov/gsafsd\\_sp?id=kb\\_article\\_view&sysparm\\_article=KB0016380&sys\\_kb\\_id=194695221bfe4d983565ed3ce54bcbbb&spa=1](https://www.fsd.gov/gsafsd_sp?id=kb_article_view&sysparm_article=KB0016380&sys_kb_id=194695221bfe4d983565ed3ce54bcbbb&spa=1)

**Please note**, guidance on SAM.gov and the guidance on GSA’s website about requirement for registering in SAM.gov is subject to change at any time. Applicants should review the website frequently for the most up-to-date guidance.

**Organizations based outside of the United States and that DO plan to do business with the DoD in addition to Department of State should follow the below instructions:**

Step 1: Apply for an NCAGE code by following the instructions on the NSPA NATO website linked below:

NCAGE Homepage:

<https://eportal.nspa.nato.int/AC135Public/sc/CageList.aspx>

NCAGE Code Request Tool (NCRT):

<https://eportal.nspa.nato.int/Codification/CageTool/home>

### D3.1 SAM.gov and UEI Exemptions

An exemption from the UEI and sam.gov registration requirements may be permitted on a case-by-case basis if:

- An applicant’s identity must be protected due to potential endangerment of their mission, their organization’s status, their employees, or individuals being served by the applicant.
- For an applicant, if the federal awarding agency makes a determination that there are exigent circumstances that prohibit the applicant from receiving a unique entity identifier and completing SAM.gov registration prior to receiving a federal award. In these instances, federal awarding agencies must require the recipient to obtain a unique entity identifier and complete SAM.gov registration within 30 days of the federal award date.

Organizations requesting exemption from UEI or SAM.gov requirements must email the point of contact listed in Section G of the NOFO at least **two weeks prior to the deadline in the NOFO providing a justification of their request**. Approval for a SAM.gov exemption must come from the warranted Grants Officer before the application can be deemed eligible for review.

### D3.2 Registering in MyGrants and Grants.gov

All application submissions must be made electronically via [Grants.gov](https://grants.gov) or MyGrants (<https://mygrants.servicenowservices.com/ilms/>). Both systems require registration by the applying organization. Please note that the Grants.gov registration process can take ten (10) business days or longer, even if all registration steps are completed in a timely manner. Instructions for registering and submitting applications in each system are provided below.

#### **MyGrants:**

Applicants using MyGrants for the first time should complete their “New Organization Registration.” To register with MyGrants, go to: <https://mygrants.servicenowservices.com> and click “create an account”.

Please note that establishing an account in MyGrants may require the use of smartphone for multi-factor authentication (MFA). If an applicant does not have accessibility to a smartphone during the time of creating an account, please contact the helpdesk and request instructions on MFA for Windows PC.

Organizations **must** remember to save a screen shot of the checklist showing all documents submitted in case any document fails to upload successfully.

#### **MyGrants Help Desk:**

For assistance with MyGrants accounts and technical issues related to the system, please contact the ILMS help desk by phone at +1 (888) 313-4567 (toll charges apply for international callers) or through the Self Service online portal that can be accessed from <https://afsism.service-now.com/ilms/home>. Customer support is available 24/7.

#### **Grants.gov:**

Applicants who do not submit applications via MyGrants may submit via [Grants.gov](https://www.grants.gov). Please be advised that completing all the necessary registration steps for obtaining a username and password from Grants.gov **can take ten (10) business days or longer**.

Please refer to the Grants.gov website for definitions of various “application statuses” and the difference between a submission receipt and a submission validation. Applicants will receive a validation e-mail from Grants.gov upon the successful submission of an application. Validation of an electronic submission via Grants.gov can take up to two business days. Additionally, organizations **must** remember to save a screenshot of the checklist showing all documents submitted in case any document fails to upload successfully.

#### **Grants.gov Helpdesk:**

For assistance with Grants.gov, please call the Contact Center at +1 (800) 518-4726 or email [support@grants.gov](mailto:support@grants.gov). The Contact Center is available 24 hours a day, seven days a week, except federal holidays. A full list of federal holidays can be found [here](#).

#### **D4. Submission Dates and Times**

Applications are due no later than **11:59 PM EST/EDT on 29 July 2024** on Grants.gov (<https://www.grants.gov/>), or MyGrants (<https://mygrants.servicenowservices.com>), under the announcement title “**Building International Data Protection and Capacity**” and funding opportunity number “DFOP0016688”.

Grants.gov and MyGrants automatically log the date and time an application submission is made, and the Department of State will use this information to determine whether an application has been submitted on time. Late applications are neither reviewed nor considered. Known system errors caused by Grants.gov or MyGrants (<https://mygrants.service-now.com>) that are outside of the applicant’s control will be reviewed on a case-by-case basis. Applicants should not expect a notification upon CDP receiving their application.

## D5. Funding Limitations, Restrictions, and other Considerations

CDP will not consider applications that reflect any type of support for any member, affiliate, or representative of a designated terrorist organization. Please refer the link for Foreign Terrorist Organizations: <https://www.state.gov/foreign-terrorist-organizations/>

Project activities whose direct beneficiaries are foreign militaries or paramilitary groups, or individuals will not be considered for CDP funding given purpose limitations on funding.

The Leahy Law prohibits Department foreign assistance funds from supporting foreign security force units if the Secretary of State has credible information that the unit has committed a gross violation of human rights. Per [22 USC §2378d\(a\) \(2017\)](#), “No assistance shall be furnished under this chapter [FOREIGN ASSISTANCE] or the Arms Export Control Act [22 USC 2751 et seq.] to any unit of the security forces of a foreign country if the Secretary of State has credible information that such unit has committed a gross violation of human rights.” Restrictions may apply to any proposed assistance to police or other law enforcement. Among these, pursuant to section 620M of the Foreign Assistance Act of 1961, as amended (FAA), no assistance provided through this funding opportunity may be furnished to any unit of the security forces of a foreign country when there is credible information that such unit has committed a gross violation of human rights. In accordance with the requirements of section 620M of the FAA, also known as the Leahy law, project beneficiaries or participants from a foreign government’s security forces may need to be vetted by the Department before the provision of any assistance. If a proposed grant or cooperative agreement will provide assistance to foreign security forces or personnel, compliance with the Leahy Law is required.

Organizations should be cognizant of these restrictions when developing project proposals as these restrictions will require appropriate due diligence of project beneficiaries and collaboration with CDP to ensure compliance with these restrictions. Project beneficiaries subject to due diligence vetting will include any individuals or entities that are beneficiaries of foreign assistance funding or support. Due diligence vetting will include a review of open-source materials.

## D6. Other Submission Requirements

It is the responsibility of the applicant to ensure that it has an active registration in MyGrants or Grants.gov. Applicants are required to document that the application has been received by MyGrants or Grants.gov in its entirety. CDP bears no responsibility for disqualification that result from applicants not being registered before the due date, for system errors in either MyGrants or Grants.gov, or other errors in the application process.

Applicants are strongly encouraged to save a screen shot of the checklist showing all documents submitted in case any document fails to upload successfully.

Faxed, couriered, or emailed documents will not be accepted. Reasonable accommodations may, in appropriate circumstances, be provided to applicants with disabilities or for security

reasons. **Applicants must follow all formatting instructions in the applicable NOFO and these instructions.**

CDP encourages organizations to **submit applications during normal business hours** (Monday – Friday, 9:00AM-5:00PM Eastern Time (EST or EDT as case may be)). If an applicant experiences technical difficulties and has contacted the appropriate helpdesk but is not receiving timely assistance (i.e., if you have not received a response within 48 hours of contacting the helpdesk), you may contact the CDP point of contact listed in in Section G for further assistance.

## Section E: Application Review Information

### E1. Proposal Review Criteria

The selected CDP review panel will evaluate each application individually against the following criteria, listed below in order of importance, and not against competing applications. Please use the below criteria as a reference, but **do not structure your application according to the sub-sections. Quality of Project Design (20 points)**

- The project idea is well developed and responsive to the policy and program objective(s) in the NOFO.
- The applicant clearly defines the problem; it's causes; stakeholders; and existing research/data; the approach taken to solve the problem; realistic milestones to indicate progress.
- The project's potential contribution to solving the problem is addressed in the problem statement.

### **Organizational Capacity (20 points)**

- The application demonstrates an institutional record of successful projects in the content area proposed and relevant experience in the proposed country/territory/region.
- The organization has expertise in its stated field and has adequate staffing to manage the proposed project.
- The application demonstrates the organization's capacity for responsible fiscal management of donor funding.

### **Project Planning and Ability to Achieve Objectives (30 points)**

- Goals and objectives are clearly stated, and project approach illustrates logical and plausible pathways to achieving project outcomes.
- Proposed project activities are feasible, practical, and/or experiential in nature to encourage innovation.
- Key assumptions and risks have been identified and their potential influences described.
- If similar activities have taken place, the applicant explains how proposed activities will produce new impact and not simply duplicate past efforts.

**Monitoring & Evaluation Plan (10 points)**

- The proposal demonstrates a sound plan for monitoring appropriate indicators to oversee the project's timely progress toward stated objectives, capture key project results, and to assess and mitigate any challenges encountered in implementation.
- Includes output and outcome indicators, explains how and when those will be measured, and by whom.

**Budget & Budget Narrative (10 points)**

- The budget justification is a detailed and realistic financial expression of the proposed project and does not include estimated costs that are not allocable, reasonable, or allowable.
- Proposed costs are linked to project objectives and demonstrate efficient use of U.S. Government funds.
- Proposal budget, including salaries and honoraria, are explained, and justified for the work involved.

**Sustainability of Impact/Multiplier Effect (10 points)**

- The proposal clearly details how project activities will produce benefits and impact lasting beyond the funding period.
- Methods to ensure sustainability of project impact beyond the life of the award are clearly delineated.

## E2. Review and Selection Process

The Department of State is committed to ensuring a competitive and standardized process for awarding funding. Applications will be screened initially in a Technical Eligibility Review stage to determine whether applicants meet the eligibility requirements outlined in section C and have submitted all required documents outlined in section D. Applications that do not meet these requirements will not advance beyond the Technical Eligibility Review stage and will be deemed ineligible for funding under this NOFO.

All applications that are deemed technically eligible will proceed to the Merit Review Panel consisting of U.S. government subject matter and/or country-specific experts and will be rated on a 100-point scale. CDP reserves the right to request the assistance of non-US government Subject Matter Experts (SMEs), if appropriate to the solicitation. Point values for individual elements of the application are presented in Section E.1. Panel Reviewers' ratings, and any resulting recommendations, are advisory. Panel Reviewers may provide conditions and recommendations on applications to enhance the proposed project, which must be addressed by the applicant before further consideration of the award.

Final selection authority resides with CDP's senior level official. Final award decisions will be influenced by whether the application meets the Department of State's programmatic goals and objectives, how it supports the Department's overarching foreign policy priorities, and the geographic distribution of the top-ranking applications.

### E3. Responsibility/Qualification Information in SAM.gov (formerly, FAPIIS)

For any federal award under a notice of funding opportunity, if the federal awarding agency anticipates that the total federal share will be greater than the simplified acquisition threshold over the period of performance (see §200.01 Simplified Acquisition Threshold), this section must also inform applicants that:

- i. The Department of State, prior to making a federal award with a total amount of federal share greater than the simplified acquisition threshold, is required to review and consider any information about the applicant that is in the designated integrity and performance system accessible through SAM.gov (see 41 U.S.C. 2313);
- ii. The applicant, at its option, may review and comment on any information about itself that a federal awarding agency previously entered. Currently, federal agencies create integrity records in the integrity module of the Contractor Performance Assessment and Reporting System (CPARS) and these records are visible as responsibility/qualification records in SAM.gov;
- iii. The Department of State will consider any comments by the applicant, in addition to the other information in the designated integrity and performance system, in making a judgment about the applicant's integrity, business ethics, and record of performance under federal awards when completing the review of risk posed by applicants as described in §200.205 - Federal awarding agency review of risk posed by applicants.

## Section F: Federal Award Administration Information

### F1. Federal Award Notices

The Bureau of Cyberspace and Digital Policy (CDP) will provide a separate notification to applicants on the result of their applications. Successful applicants will receive a letter electronically via email including a request for the applicant respond to panel conditions and recommendations. This notification is **not** an authorization to begin activities and does not constitute formal approval or a funding commitment.

Final approval is contingent on the applicant successfully responding to the merit review panel's conditions and recommendations; being registered in required systems; and providing any additional completed documentation requested by CDP or the Grants Officer. Final approval is also contingent on Congressional Notification requirements being met and final review and approval by the Department's warranted Grants Officer.

The Notice of Award signed by the Department's warranted Grants Officers is the sole authorizing document. The recipient may only start incurring project expenses beginning on the start date shown on the grant award document signed by the Grants Officer. If awarded, the Notice of Award will be provided to the applicant's designated Authorizing Official via MyGrants to be electronically counter signed in the system.

Payments under this award will be made through the U.S. Department of Health and Human Services (HHS) Payment Management System (PMS). Unless otherwise stipulated, the Recipient

may request payments on a reimbursement or advance basis. Instructions for requesting payments are available at: <https://pms.psc.gov/>.

Advance payments must be limited to the minimum amounts needed and be timed to be in accordance with the actual, immediate cash requirements of the Recipient in carrying out the purpose of this award. The timing and amount of advance payments must be as close as is administratively feasible to the actual disbursements by the Recipient for direct program or project costs and the proportionate share of any allowable indirect costs.

## F2. Administrative, National Policy and Legal Requirements

Legal restrictions on foreign assistance are regularly updated. The CDP Bureau requires all recipients of foreign assistance funding to comply with all applicable Department and federal laws and regulations, including but not limited to the following:

The Uniform Administrative Requirements, Cost Principles and Audit Requirements for Federal Awards set forth in 2 CFR Chapter 200 (Sub-Chapters A through F) shall apply to all non-federal entities, except for assistance awards to Individuals and Foreign Public Entities. Sub-Chapters A through E shall apply to all foreign organizations, and Sub-Chapters A through D shall apply to all U.S. and foreign for-profit entities. The applicant/recipient of the award and any sub-recipient under the award must comply with all applicable terms and conditions, in addition to the assurance and certifications made part of the Notice of Award. The Department's Standard Terms and Conditions can be viewed at <https://www.state.gov/about-us-office-of-the-procurement-executive/>.

Before submitting an application, applicants should review all the terms and conditions and required certifications which will apply to this award, to ensure that they will be able to comply. These include:

- [2 CFR 25 – UNIVERSAL IDENTIFIER AND SYSTEM FOR AWARD MANAGEMENT](#)
- [2 CFR 170 – REPORTING SUBAWARD AND EXECUTIVE COMPENSATION INFORMATION](#)
- [2 CFR 175 – AWARD TERM FOR TRAFFICKING IN PERSONS](#)
- [2 CFR 182 – GOVERNMENTWIDE REQUIREMENTS FOR DRUG-FREE WORKPLACE \(FINANCIAL ASSISTANCE\)](#)
- [2 CFR 183 – NEVER CONTRACT WITH THE ENEMY](#)
- [2 CFR 600 – DEPARTMENT OF STATE REQUIREMENTS](#)
- [U.S. DEPARTMENT OF STATE STANDARD TERMS AND CONDITIONS](#)

In accordance with the Office of Management and Budget's guidance located at 2 CFR part 200, all applicable federal laws, and relevant Executive guidance, the Department of State will review and consider applications for funding, as applicable to specific programs, pursuant to this notice of funding opportunity in accordance with the following:

- [Guidance for Grants and Agreements in Title 2 of the Code of Federal Regulations](#) (2 CFR), as updated in the Federal Register’s 85 FR 49506 on August 13, 2020, particularly on:
  - Selecting recipients most likely to be successful in delivering results based on the project objectives through an objective process of evaluating federal award applications (2 CFR part 200.205),
  - Prohibiting the purchase of certain telecommunication and video surveillance services or equipment in alignment with section 889 of the National Defense Authorization Act of 2019 (Pub. L. No. 115—232) (2 CFR part 200.216),
  - Promoting the freedom of speech and religious liberty in alignment with *Promoting Free Speech and Religious Liberty* (E.O. 13798) and *Improving Free Inquiry, Transparency, and Accountability at Colleges and Universities* (E.O. 13864) (§§ 200.300, 200.303, 200.339, and 200.341),
  - Providing a preference, to the extent permitted by law, to maximize use of goods, products, and materials produced in the United States (2 CFR part 200.322), and
  - Terminating agreements in whole or in part to the greatest extent authorized by law if an award no longer effectuates the program goals or agency priorities (2 CFR part 200.340).

### F3. Reporting

Reporting is critical to effective project management and oversight. Reports are required as a means of evaluating the recipient’s progress and utilization of resources. They are divided between a performance progress report and a financial status report. Applicants should be aware that CDP awards require that all reports (progress and financial) are uploaded to the grant file in MyGrants typically on a quarterly basis. The Federal Financial Report (FFR or SF-425) is the required form for the financial reports and must be submitted in PMS, as well as a copy from PMS then uploaded to the grant file in MyGrants. The progress reports uploaded to the grant file in MyGrants must include a narrative as described below and project indicators (or other mutually agreed upon format approved by the Grants Officer) for the F Framework and DCCP indicators. The F Framework indicators and DCCP indicators will be reviewed and negotiated during the final stages of issuing an award.

**Financial Reports** are also required on a quarterly basis (unless stipulated otherwise in the final Agreement), using form SF-425, the Federal Financial Report form. If payment is made through the Payment Management System, all financial reports must be submitted electronically through the Payment Management System. The Recipient is also required to upload to MyGrants a pdf version of all financial reports (Federal Financial Report) they have submitted in the Payment Management System. Form (SF-425) is located on the Post-Award Reporting forms page of [Grants.gov](https://www.grants.gov), linked here.

### Final Reports

The final report will be due no later than 120 days after the end date of the award or termination of all project activities. The final report shall include the following elements:

executive summary, successes, outcomes, best practices, how the project will be sustained, and a final Federal Financial Report (FFR). Additional guidance may be provided prior to the award end date.

*Please note*, delays in reporting may result in delays of payment approvals and failure to provide required reports may jeopardize the recipients' ability to receive future U.S. government funds. CDP reserves the right to request any additional programmatic and/or financial project information during the award period of performance.

### **Foreign Assistance Data Review (FADR)**

As required by Congress, the Department of State must make progress in its efforts to improve tracking and reporting of foreign assistance data through the Foreign Assistance Data Review (FADR). The FADR requires tracking of foreign assistance activity data from budgeting, planning, and allocation through obligation and disbursement. Successful applicants will be required to report and draw down federal funding based on the appropriate FADR Data Elements, indicated within their award documentation. In cases of more than one FADR Data Element, typically program or sector and/or regions or country, the successful applicant will be required to maintain separate accounting records.

Applicants should be aware of the post award reporting requirements reflected in [2 CFR 200 Appendix XII—Award Term and Condition for Recipient Integrity and Performance Matters](#).

## Section G: Federal Awarding Agency Contacts

For technical submission questions related to this NOFO, please contact:

DCCP Foreign Assistance Team  
Digital Connectivity and Cybersecurity Partnership (DCCP)  
Unit of Strategic Planning and Communications (SPC)  
Bureau of Cybersecurity and Digital Policy (CDP)  
[DCCP-Info@state.gov](mailto:DCCP-Info@state.gov)

### G1. Questions

Any prospective applicant who has questions concerning the contents of this NOFO must email the questions to the contacts listed above with the subject “**Building International Data Protection and Capacity**.” To maintain fairness and transparency in competition, CDP will not answer substantive NOFO questions except when posting questions and answers to the announcement page as described below.

All questions must be submitted via email to contacts listed above by the deadline stated on page 3. CDP will periodically create a document of submitted questions with answers and upload it and post them in grants.gov. Prospective applicants are advised to regularly review

the announcement page in grants.gov for any updates. Note that once the NOFO deadline has passed, DOS staff in Washington, D.C. may not discuss this completion with applicants until the review process has been completed.

## Section H: Other Information

Applicants should be aware that CDP understands that some information contained in applications may be considered sensitive or proprietary and will make appropriate efforts to protect such information. However, applicants are advised that Department of State cannot guarantee that such information will not be disclosed, including pursuant to the Freedom of Information Act (FOIA) or other similar statutes.

The information in this NOFO is binding and may not be modified by any CDP representative. Explanatory information provided by CDP that contradicts this language will not be binding. Issuance of this NOFO does not constitute an award commitment on the part of the U.S. government, nor does it commit the U.S. government to pay for costs incurred in the preparation and submission of proposals. Further, the U.S. government reserves the right to reject any or all proposals received.

In accordance with applicable federal awarding agency policy, applicants must disclose in writing any potential conflict of interest to the federal awarding agency or pass-through entity.

If an award is issued, the award recipient will receive the DCCP Messaging Manual and will be required to adhere to all relevant branding requirements identified therein, including style guidelines (consistent with U.S. Department of State style guidelines), branding and logo information, and other important references and resources for DCCP partners.

Additional background information on CDP and its efforts can be found on:

<https://www.state.gov/bureaus-offices/deputy-secretary-of-state/bureau-of-cyberspace-and-digital-policy/>.

### **Attachments:**

1. **Tab 1 Building International Data Protection and Capacity** *Scope of Work Template*
2. **Tab 2 Building International Data Protection and Capacity** *Project Logic Model Template*
3. **Tab 3 Building International Data Protection and Capacity** *Performance Monitoring and Evaluation Plan Template*
4. **Tab 4 Building International Data Protection and Capacity** *Detailed Budget Template*
5. **Tab 5 Building International Data Protection and Capacity** *Budget Narrative Template*

