

U.S. Department of State
Bureau of International Security and Nonproliferation, Office of Cooperative Threat
Reduction (ISN/CTR)
Notice of Funding Opportunity

Funding Opportunity Title:	Countering Russian Chemical and Biological Threats (RCBT)
Funding Opportunity Number:	SFOP0010111
Deadline for Applications:	January 31, 2024 11:59PM EDT
CFDA Number:	19.033
Total Amount Available:	\$12,000,000

A. PROGRAM DESCRIPTION

The Department of State's Bureau of International Security and Nonproliferation, Office of Cooperative Threat Reduction (ISN/CTR) is pleased to announce an open competition for assistance awards through this Notice of Funding Opportunity (NOFO). ISN/CTR sponsors foreign assistance activities funded by the Nonproliferation, Antiterrorism, Demining and Related Programs (NADR) and other accounts and focuses on mitigating weapons of mass destruction (WMD) and WMD-related delivery systems proliferation and security threats from non-state actors and proliferator states.

ISN/CTR's Countering Russian Chemical and Biological Threats (C-RCBT) program supports efforts by the U.S. and its allies to help identify and inhibit Russian WMD proliferation programs. The world has witnessed high-profile Russian assassination attempts utilizing chemical weapons - including the 2018 attempted murder of Sergei Skripal and his daughter in the U.K., and the 2020 attempt against Aleksey Navalny in Russia. Consequently, the United States has issued a range of sanctions and designations in response to Russia's proliferation and dissemination activities. Specifically, the U.S. Department of Commerce has publicly identified at least 19 Russian and Russian-linked entities that are believed to be associated with Russian chemical and biological weapons programs. Additionally, the U.S. Departments of Treasury and State have also designated Russian-linked entities associated with Russian chemical weapons development. To advance its chemical and biological weapons (CBW) proliferation efforts, the Russian Federation has developed intentionally complex procurement and beneficial ownership networks.

ISN/CTR's C-RCBT program seeks to prevent Russian Federation access to advanced dual-use equipment, materials, and knowledge that could advance Russian chemical and biological proliferation threats. The C-RCBT program seeks to constrain Russian proliferation activities by training law enforcement and security officials, government watchdogs and regulators, Fortune 500 companies, private sector biological, biotechnology, biomedical, chemical, scientific equipment and supplies, and pharmaceutical (BBCP) compliance and legal specialists, manufacturers, distributors, and logistics providers, financiers, and scientists on the reputational, sanctions, and financial risks of engaging with Russian proliferation networks.

Additionally, an important element in highlighting Russian proliferation networks is to identify and address associated financial, logistics, and facilitation networks (e.g., front companies, third party brokers, and other obfuscation methods) that may inadvertently aid Russian proliferation. This is especially important in an era of increased public awareness of this Russian threat, and the growing sanctions, financial, and reputational risks for the private sector in engaging directly or indirectly with designated Russian entities.

A recent ISN/CTR supported report analyzing commercial data involving 10 entities linked to Russian WMD proliferation identified more than 30,100 direct transactions since these entities were designated between August 2020 - March 2021 through August 31, 2023. These transactions were worth more than \$72 million USD and occurred in over 30 countries around the world – including throughout Western Europe. Concerningly, commercially-available data identified a significant number of transactions between Russian-linked WMD entities and well-known Fortune 500 companies – demonstrating a critical need to raise awareness in the private and enforcement sectors to avoid sanctions, financial, and reputational risks.

The C-RCBT program seeks to raise awareness, enhance capacity, and protect critical infrastructure and scientific networks from Russian exploitation for WMD proliferation purposes.

ISN/CTR's C-RCBT program efforts involve engagement, development, and implementation of projects to advance one or more of the following objectives:

- Develop and disseminate reports that leverage commercially available data in order to support actionable and targeted capacity-building for the biological, biotech, biomedical, chemical, scientific equipment and supplies, and pharmaceutical sectors that illuminate procurement, financial, and logistics networks that Russia exploits for proliferation purposes.
- Enhance partner public and private sector capacity and coordination to inhibit illicit procurement networks, supply chains, and transshipment through partner states being exploited by Russian proliferation procurement pathways, including the financing mechanisms behind them.
- Support peer-to-peer engagements, including with Fortune 500 companies and the biotech and pharmaceutical sectors, to help enhance capacity to reduce financial, sanctions, and reputational risks.
- Strengthen awareness, best practices, risk awareness and monitoring networks and communities of practice for traditional and non-traditional partners to protect expertise, research collaboration, and tacit knowledge from exploitation by Russia for proliferation purposes.

Program Objectives:

ISN/CTR seeks programmatic proposals supporting the following lines of effort (LOEs):

- 1. Develop and Disseminate Commercially-Available Data and Analyses That Highlight Illicit Russian Proliferation, Procurement, and Facilitation Networks in the Global Supply Chain:** ISN/CTR leverages open-source, and commercially available data to identify actionable information for private sector compliance and public sector enforcement entities on Russian chemical and biological proliferation and procurement activities. These projects focus on highlighting Russian attempts to access dual-use equipment, supplies, and other materials that could be misused for proliferation purposes. It includes analysis on direct and indirect procurement, financial, and logistics transactions in the global supply chain. Additionally, these efforts seek to highlight Russian networks that attempt to exploit scientific collaborations and exchanges to advance proliferation efforts.

ISN/CTR programs seek to provide actionable and commercially-available data for foreign private sector compliance officials (including those from Fortune 500 companies) and public sector enforcement officials on Russian proliferation networks in the global supply chain. This data will also be provided to legal, sales, manufacturing, distribution, logistics, and compliance officials in the biological, biotech, biomedical, chemical, scientific equipment and supplies, and pharmaceutical sectors.

This analysis focuses on direct and indirect transactions on over 19 Russian and Russian-linked entities publicly identified by the U.S. Departments of Commerce, State, and Treasury that are believed to be associated with Russian biological and chemical weapons programs.

The C-RCBT program area is seeking projects that will:

- Leverage open-source and commercially available data to identify actionable information on Russian procurement networks involving the BBCP sectors and the financing behind them.
- Provide up-to-date commercially available trade analysis of the more than 19 entities publicly identified to be linked to Russian WMD proliferation activities.
- Leverage commercially available data to build out network typologies to help identify additional high-risk entities and obfuscated networks.
- Employ data research and analytics firms to highlight transactions involving designated Russian and Russian-linked entities.
- Support industry experts, especially from the business risk and the BBCP compliance community, to leverage commercially available reports to demonstrate direct and indirect risks to engage private sector compliance, sales, manufacturers, suppliers, and distributors.
- Provide open-source data that can assist in enhancing due diligence, know your customer (and customer's customer), and list-based compliance best practices to strengthen corporate risk-mitigation protocols.
- Utilize existing commercial or collaborative networks to facilitate expert engagements and dissemination of analysis, datasets, and information.

- Protect the academic and research community from exploitation by Russian proliferation networks by conducting open-source analysis to identify and mitigate against vulnerabilities.

Please note: The C-RCBT Program does not fund long-term research projects or the development of new analytical tools or software. ISN/CTR does not seek to acquire an in-house data analytical tool, nor training for ISN/CTR or other USG staff to operate such tools. Further, the C-RCBT Program does not fund subscription services to existing publicly available data analytics tools for foreign partners, given the lack of long-term sustainability inherent in such efforts. Instead, ISN/CTR seeks to build sustainable partner country appetite and capacity to meet their own open-source data needs for CBW counterproliferation purposes.

Geographic Focus: EUR, SCA, EAP, global (limited)

Compliance/Legal: Austria, Belgium, Brazil, Canada, Cyprus, Finland, France, Germany, India, Italy, Ireland, Japan, Lithuania, Luxembourg, Netherlands, Norway, Poland, Spain, Sweden, Switzerland, Republic of Korea, Singapore, Taiwan, Türkiye, United Kingdom.

Manufacturing: Austria, Azerbaijan, Brazil, Belgium, Canada, Cyprus, Finland, France, Germany, Hungary, India, Indonesia, Italy, Ireland, Japan, Kazakhstan, Lithuania, Luxembourg, Malaysia, Netherlands, Norway, Poland, Republic of Korea, Singapore, Spain, Sweden, Switzerland, Taiwan, Türkiye, United Kingdom, Vietnam.

Distribution: Azerbaijan, Czechia, Cyprus, Estonia, Hungary, India, Indonesia, Japan, Kazakhstan, Latvia, Lithuania, Malaysia, Moldova, Poland, Republic of Korea, Romania, Singapore, Slovakia, Taiwan, Türkiye, Vietnam.

Financing: Cyprus, France, Germany, India, Luxembourg, Singapore, Spain, Switzerland, Taiwan, Türkiye, United Kingdom.

2. **Enhancing Private and Public Sector Due Diligence to Identify and Inhibit Russian Exploitation of Global BBCP Supply Chain:** This LOE enhances partner countries' capacity to identify and avoid financial, sanctions, and reputational risks of engaging Russian proliferation networks through capacity building to enhance due-diligence. The efforts will raise awareness in the BBCP private sector and public enforcement sector on risks of unwittingly engaging obfuscated Russian proliferation networks, and the open-source tools and best-practices available to enhance due-diligence. This LOE seeks to facilitate public-private partnerships through training, seminar, table-top exercises, and business risk consultations to strengthen list-based compliance, Know-Your-Customer (and Customer's Customer), and other risk mitigation best-practices. Previous engagements have highlighted the more than 19 sites that the United States has publicly identified to be associated with the Russian WMD program.

The RCBT program area is seeking FY2024 projects that will:

- Support industry experts, especially from the business risk and the BBCP compliance community, to engage private sector compliance, sales, manufacturers, suppliers, and distributors.
- Support peer-to-peer interactions between well-known financial and business consultation firms with Fortune 500 companies and the broader BBCP community.
- Enhance due diligence, know your customer (and customer's customer), and list-based compliance best practices to strengthen corporate risk-mitigation protocols.
- Provide open-source materials, trainings, and other tools to strengthen compliance and due-diligence best-practices.
- Provide capacity building trainings for industry and governmental stakeholders to enable them to identify illicit Russian procurement activities in the BBCP global supply chains and related financing and logistics.
- Empower partner industry and government stakeholders through training, tabletop exercises, risk assessment methodologies, and information sharing to develop best practices to protect from sanctions, financial, and reputational risks.
- Build like-minded BBCP communities and networks in order to help secure BBCP supply chains from exploitation by Russian proliferation programs.
- Facilitate public-private partnerships to prevent becoming entwined with illicit procurement networks.
- Provide 'Know Your Customer,' due diligence, and risk management best practices training for manufacturers, distributors and shippers of dual-use materials and equipment to prevent exploitation for proliferation purposes.
- Leverage open-source and commercially available data to provide actionable information on Russian illicit procurement activities within the global BBCP community and related enforcement entities.
- Support a holistic approach that includes engaging the entire BBCP supply chain from manufacturers, sales, distribution, logistics, legal, and compliance.
- Train BBCP compliance specialists how to conduct their own open-source research, KYC checks, and due diligence – including illicit procurement activities via transshipment points, shell companies, or other locations or mechanisms that may be deliberately obfuscating their true malign intention.
- Engage those in the BBCP supply chain involved in managing transactions to and through transshipment points (e.g., distribution, logistics, shipping and freight forwarders).
- Employ a region, country, sector, and audience-specific approach.
- Include training on cybersecurity protection in the BBCP supply chain.

This LOE particularly seeks creative, cost-effective, sustainable engagements that leverage train-the-trainer, regional champions, and other self-led engagements by foreign partners. They could also include targeted capstone activities, tailored

consultations, discrete follow-on activities, and/or mentorship models to help maximize impact.

Geographic Focus: EUR, SCA, EAP, global (limited)

Compliance/Legal: Austria, Belgium, Brazil, Canada, Cyprus, Finland, France, Germany, India; Italy, Japan, Lithuania, Luxembourg, Netherlands, Norway, Poland, Republic of Korea Singapore, Spain, Sweden, Switzerland, Taiwan, Türkiye, United Kingdom.

Manufacturing: Austria, Azerbaijan, Brazil, Belgium, Canada, Cyprus, Finland, France, Germany, Hungary, India, Indonesia, Italy, Japan, Kazakhstan, Lithuania, Malaysia, Moldova, Netherlands, Norway, Poland, Republic of Korea, Singapore, Spain, Sweden, Switzerland, Türkiye, United Kingdom.

Distribution: Azerbaijan, Czechia, Cyprus, Estonia, Hungary, India, Indonesia, Kazakhstan, Japan, Latvia, Lithuania, Luxembourg, Malaysia, Moldova, Poland, Republic of Korea, Romania, Slovakia, Taiwan, Türkiye, Vietnam.

Financing: Cyprus, France, India Luxembourg, Germany, Spain, Singapore, Switzerland, Taiwan, Türkiye, United Kingdom.

3. **Enhancing Due-Diligence in the Scientific Community:** This LOE increases awareness in the scientific, academic, research, and funding communities on the challenges posed by illicit Russian proliferation networks seeking to exploit dual-use equipment, materials, and knowledge. This program focuses on establishing peer-peer information-sharing networks to promote due diligence among research institutes, academic communities, and other scientific and government stakeholders with equities in the BBCE sectors. Importantly this includes an increasing focus on international funding agencies (e.g., charities, nonprofits) to strengthen due-diligence practices and prevent unwitting ties to proliferation activities.

Previous work included training public and private life science and biotechnology researchers from academia, laboratories, and research institutes with a focus on identifying best practices to protect research, knowledge, and funding. Participants developed country-specific action plans to increase coordination between traditional and non-traditional partners to support further dissemination of best-practices regionally.

The RCBT program area is seeking FY2023 projects that will:

- Engage industry, academic, public and private research institute partners to promote dual-use best practices.
- Raise awareness of Russian proliferation activities and networks, and the risks of doing business with sanctioned, designated, or otherwise high-risk entities.
- Build networks among universities, research institutes, industry and non-traditional partners such as academic specialty and funding bodies to prevent exploitation of legitimate scientific endeavors by proliferator states.

- Develop creative approaches for identifying and engaging non-traditional partners such as academic specialty and funding bodies in awareness-raising, networking, and capacity building to enhance due-diligence.
- Identify, promote, and implement practitioner-driven best practices, including on cybersecurity, to protect tacit knowledge and expertise from exploitation for proliferation purposes.

This LOE seeks creative, cost-effective, and self-sustaining approaches to promulgate, implement, reinforce and strengthen mechanisms, policies and procedures that protect research collaborations. Typical projects promote best practices on KYC, policies, and sub-regulatory measures for widespread adoption of enhanced due diligence.

Geographic Focus:

EAP: Indonesia, Malaysia, Singapore, Taiwan, Vietnam

EUR: Azerbaijan, Cyprus, Estonia, France, Germany, Italy, Latvia, Lithuania, Luxembourg, Moldova, Montenegro, Netherlands, Poland, Slovakia, Spain, Türkiye, Switzerland, United Kingdom

SCA: India, Kazakhstan

B. FEDERAL AWARD INFORMATION

Length of Performance Period: Twelve (12) months

Award Amounts: Awards should typically range between \$50,000 to \$300,000 per project

Total available funding: \$12,000,000

Type of Funding: FY24/25 Nonproliferation, Anti-Terrorism, Demining and Related Activities Funds under the Foreign Assistance Act.

Anticipated Project Start Date: October 1, 2024

Funding Instrument Type: Cooperative agreement. Cooperative agreements are different from grants in that bureau staff are more actively involved in the grant implementation. CTR will play an active role in developing and shaping the materials developed and implanted during this award. CTR will also help identify participants.

Project Performance Period: Proposed projects should be completed in 12 months or less.

This notice is subject to availability of funding.

C. ELIGIBILITY INFORMATION

1. Eligible Applicants

The following organizations are eligible to apply:

- Not-for-profit organizations, including think tanks and civil society/non-governmental organizations
- Public and private educational institutions
- Federally funded research and development centers (FFRDCs)
- For-profit organizations Public International Organizations and Governmental institutions

2. Cost Sharing or Matching

Cost sharing is not required and will play no role in when the project is being evaluated.

3. Other Eligibility Requirements

In order to be eligible to receive an award, all organizations must have a Unique Entity Identifier (UEI) number issued via www.SAM.gov as well as a valid registration on www.SAM.gov. Please see Section D.3 for more information.

Applicants are only allowed to submit one proposal package per organization. If more than one proposal package is submitted from an organization, all proposals from that institution may be considered ineligible for funding.

D. APPLICATION AND SUBMISSION INFORMATION

1. Address to Request Application Package

Required application forms are available at grants.gov.

2. Content and Form of Application Submission

Please follow all instructions below carefully. Proposals that do not meet the requirements of this announcement or fail to comply with the stated requirements will be ineligible.

Content of Application

Please ensure:

- The proposal clearly addresses the goals and objectives of this funding opportunity.
- All documents are in English
- All budgets are in U.S. dollars
- 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.

Proposal documents

Mandatory documents

- **SF-424 (*Application for Federal Assistance – organizations*)**
- **Project Proposal:** Please follow the directions to complete the proposal template included in the application package.
- **Consolidated Project List**
- **Budget Detail**

Optional documents

- **SF-424B (*Only required for organizations not registered in SAM.gov*)**
- **SF -LLL (DISCLOSURE OF LOBBYING ACTIVITIES)**
- **Copy of most recent approved NICRA**
- **Summary Page**
- **DEIA standalone document (Separate from DEIA plan information included in project proposal)**

2. Summary Page: Cover sheet stating the applicant name and organization, proposal date, program title, program period proposed start and end date, and brief purpose of the program.

3. Proposal (3 pages per project maximum): The proposal should contain sufficient information that anyone not familiar with it would understand exactly what the applicant wants to do. Use the project proposals template posted with this NOFO.

5. Budget Detail: Use the spreadsheet template included with the NOFO to describe each of the budget expenses in detail. See section *H. Other Information: Guidelines for Budget Submissions* below for further information.

6. Consolidated Project List: Please use the provided template to identify all key information about the project. Each project included with this proposal should have its own line on the spreadsheet.

7. Attachments (Optional)

- 1-page CV or resume of key personnel who are proposed for the program
- If your organization has a Negotiated Indirect Cost Rate Agreement (NICRA) and includes NICRA charges in the budget, your latest NICRA should be included as a PDF file.
- Standalone DEIA Statement in compliance with the optional proposal document, format included in with the guidance posted with the NOFO.
- SF-LLL form

3. Unique Entity Identifier and System for Award Management (SAM.gov)
(NOTE: This section is required and not optional.)

Required Registrations:

All organizations, whether based in the United States or in another country, must have a Unique Entity Identifier (UEI) and an active registration with the 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.

Note: As of April 2022, a DUNS number is no longer required for federal assistance applications.

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.

- 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 prior to registering in SAM.gov.
- Organizations **based outside of the United States** and that do not pay employees within the United States do not need an EIN from the IRS but do need a UEI number prior to registering in SAM.gov.
- **Please note that as of November 2022 and February 2022 respectively, organizations based outside of the United States that do not intend to apply for U.S. Department of Defense (DoD) awards are no longer required to have a NATO Commercial and Government Entity (NCAGE) code or CAGE code to apply for non-DoD foreign assistance funding opportunities.** If an applicant organization is mid-registration and wishes to remove a CAGE or NCAGE code from their SAM.gov registration, the applicant should [submit a help desk ticket](#) (“incident”) with the Federal Service Desk (FSD) online at www.fsd.gov using the following language: “I do not intend to seek financial assistance from the Department of Defense. I do not wish to obtain a CAGE or NCAGE code. I understand that I will need to submit my registration after this incident is resolved in order to have my registration activated.”

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.

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):

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 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 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 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.

4. Submission Dates and Times

Applications are due no later than **31 January 2024 at 11:59pm (EDT)**.

5. Funding Restrictions

Legal restrictions prevent ISN/CTR from providing assistance to Burma, China, Cuba, Iran, North Korea, South Sudan, Sudan, and Syria.

Under Section 635b of the Foreign Assistance Act, CTR is able to provide awards to for-profit corporations, so long as the for profit does not benefit in profit from the implementation of the award.

6. Other Submission Requirements

All application materials must be submitted through www.Grants.gov unless you are a U.S. Government entity applying for Inter-Agency Agreement (IAA) funding. If you are applying for an IAA please submit proposals to the relevant program team and ISN-CTR-BUDGET@state.gov.

E. APPLICATION REVIEW INFORMATION

1. Criteria

Applicants should note that the following criteria serve as a standard against which all project proposals will be evaluated and identify significant considerations that should be addressed in all proposals. ISN/CTR will award a cooperative agreement to the applicant(s) whose offer represents the best overall value to the government from both a technical and cost perspective.

ISN/CTR will evaluate proposals against the stated criteria. Criteria are listed in descending order of importance.

- **Proposed Activity or Activities:** Applicants should clearly describe what they propose to do and how they will do it. The proposed project(s) must directly relate to meeting the specified objectives and applicants should include specific information on how they will systematically meet ISN/CTR's global threat reduction mission. ISN/CTR will evaluate the project proposal in terms of how well it addresses the issues at hand, relevance and feasibility of the proposed activities, the timeline for completion, and the extent to which the impact of the project will continue beyond the conclusion of the period of performance.
- **Organizational Capability:** Applicants must demonstrate how their resources, capabilities, and experience will enable them to achieve the stated goals and objectives in an international technical context. The proposal(s) must identify all key partners and organizations that will be involved in implementation of this project.
- **Budget:** Proposed costs will be evaluated for feasibility, fiscal control practices, and efficiency. ISN/CTR must be able to determine that proposed costs are reasonable, allowable, and allocable to the proposed project activities. ISN/CTR will evaluate the budget to determine if the overall costs are realistic for the work to be performed, if the costs reflect the applicant's understanding of the allowable cost principles established by 2CFR200, and if the costs are consistent with the program narrative.
- **Impactful and Measurable Engagements:** Although complex nonproliferation objectives demand persistent engagement with partner countries, discrete projects should individually advance progress toward a particular objective. Proposals should describe the end-state the project aims to achieve, along with specific, measurable, and realistic benchmarks by which to gauge progress toward that end state. Compelling project proposals will

establish milestones to be met during the implementation period, and describe observable progress in meeting the program goals described above.

- **Diversity and Inclusion:** ISN/CTR values collaboration and promotes diversity, equity, and inclusion with all stakeholders by creating an environment that is open to equal opportunities without regard to race, color, religion, sex, sexual orientation, gender identity, national origin, protected veteran or disabled status. Implementers are welcome but not required to submit with their proposal a plan for how the implementer intends to further ISN/CTR's diversity, equity, inclusion, and accessibility (DEIA) objectives through their programming. Submitted plans will be evaluated separate to the overall evaluation of projects and

- **Cyber Security:** Implementer shall be required to establish and follow policy and procedures for an effective implementation of security controls using NIST 800-53 (Rev. 5 or higher)), System and Information Integrity Policy (SI-1) as follows:

- a. Identification and Authentication: Implement multifactor authentication for network access and local access.
- b. Access Controls: Implement security controls for information sharing, remote access and wireless access including: Monitoring, controlling, and protecting remote and wireless access to information by auditing information systems components (e.g., workstations, notebook computers, smartphones, and tablets).
- c. Incident Handling: Monitor and report any and all security incidents including breaches to ISN/CTR directly within 48 hours of the incident and include a risk assessment of the security access controls.

2. Review and Selection Process

A review committee will evaluate all eligible applications, final funding decision will be made by ISN/CTR Office Director and Deputy Director.

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

- i. The Federal awarding agency, 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 U.S. government designated integrity and performance system accessible through SAM.gov (see 41 U.S.C. 2313);
- ii. An 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 Federal awarding agency 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 §200.206 Federal awarding agency review of risk posed by applicants.

F. FEDERAL AWARD ADMINISTRATION INFORMATION

1. Federal Award Notices

The grant award or cooperative agreement will be written, signed, awarded, and administered by the Grants Officer. The assistance award agreement is the authorizing document and it will be provided to the recipient for review and signature by email. The recipient may only start incurring program expenses beginning on the start date shown on the grant award document signed by the Grants Officer.

If a proposal is selected for funding, the Department of State has no obligation to provide any additional future funding. Renewal of an award to increase funding or extend the period of performance is at the discretion of the Department of State.

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.

Payment Method: Payment Management System or SF-270 on a monthly basis.

2. Administrative and National Policy Requirements

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](#)
- [41 USC 4712 - Enhancement of contractor protection from reprisal for disclosure of certain information](#)
- [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: NOTE:

- [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 program 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).

In accordance with the [Executive Order on Advancing Racial Equity and Underserved Communities](#), proposals should demonstrate how the program advances equity with respect to race, ethnicity, religion, income, geography, gender identity, sexual orientation, and disability. The proposal should also demonstrate how the program will further engagement in underserved communities and with individuals from underserved communities. Proposals should demonstrate how addressing racial equity and underserved communities will enhance the program's goals and objectives, as well as the experience of participants.

The support of underserved communities will be part of the review criteria for this opportunity. Therefore, proposals should clearly demonstrate how the program will

support and advance equity and engage underserved communities in program administration, design, and implementation.

3. Reporting

Reporting Requirements: Recipients will be required to submit financial reports and program reports. The award document will specify how often these reports must be submitted.

Foreign Assistance Data Review: 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](#).

G. FEDERAL AWARDING AGENCY CONTACTS

For programmatic questions about this solicitation, contact:

Special Projects Program
Office of Cooperative Threat Reduction
U.S. Department of State
Email: ISN-CTR-SP@state.gov

Direct any NOFO submission (non-programmatic) questions to:
Office of Cooperative Threat Reduction Budget Team ISN-CTR-BUDGET@state.gov

H. OTHER INFORMATION

Guidelines for Budget Justification

Personnel and Fringe Benefits: Describe the wages, salaries, and benefits of temporary or permanent staff who will be working directly for the applicant on the program, and the percentage of their time that will be spent on the program.

Travel: Estimate the costs of travel and per diem for this program, for program staff, consultants or speakers, and participants/beneficiaries. If the program involves international travel, include a brief statement of justification for that travel.

Equipment: Describe any machinery, furniture, or other personal property that is required for the program, which has a useful life of more than one year (or a life longer than the duration of the program), and costs at least \$5,000 per unit.

Supplies: List and describe all the items and materials, including any computer devices, that are needed for the program. If an item costs more than \$5,000 per unit, then put it in the budget under Equipment.

Contractual: Describe goods and services that the applicant plans to acquire through a contract with a vendor. Also describe any sub-awards to non-profit partners that will help carry out the program activities.

Other Direct Costs: Describe other costs directly associated with the program, which do not fit in the other categories. For example, shipping costs for materials and equipment or applicable taxes. All "Other" or "Miscellaneous" expenses must be itemized and explained.

Indirect Costs: These are costs that cannot be linked directly to the program activities, such as overhead costs needed to help keep the organization operating. If your organization has a Negotiated Indirect Cost Rate (NICRA) and includes NICRA charges in the budget, attach a copy of your latest NICRA. Organizations that have never had a NICRA may request indirect costs of 10% of modified total direct costs as defined in 2 CFR 200.68.

"Cost Sharing" refers to contributions from the organization or other entities other than the U.S. Embassy. It also includes in-kind contributions such as volunteers' time and donated venues.

Alcoholic Beverages: Please note that award funds cannot be used for alcoholic beverages.