

**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
Funding Opportunity Number:	SFOP0008421
Deadline for Applications:	January 31, 2022 11:59PM EST
CFDA Number:	19.033
Total Amount Available:	\$2,000,000

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) account, and focuses on mitigating weapons of mass destruction (WMD), related delivery systems, and advanced conventional weapons proliferation and security threats from proliferator states and nonstate actors.

The United States has determined that Russia is in non-compliance with the Chemical Weapons Convention, as indicated by its use of nerve agent in the poisonings of Sergei Skripal and Alexey Navalny, Russia retains an undeclared chemical weapons program. The United States has also concluded that the Russian Federation has failed to fulfill its Article II obligation to destroy or to divert to peaceful purposes and assessed that Russia maintained an offensive biological weapons program in violation of Article I of the Convention.

ISN/CTR's Special Projects (SP) Team works to protect the exploitation of dual-use material, equipment, technology, knowledge, and expertise at government, commercial, and scientific institutions to prevent the proliferation of WMDs. Proliferators often attempt to procure sensitive equipment and technologies from unsuspecting or indiscriminate commercial or scientific institutions, subvert or otherwise undermine international nonproliferation regimes, manipulate or leverage sensitive dual-use scientific expertise, and/or seek to acquire dangerous pathogens and weaponizable materials. Russian Government-linked networks have also been perpetrating malign cyber activities targeting global institutions. These include purported Information Communication Technology attacks against supply chains, logistics firms, and biotech and pharmaceutical companies.

Finally, the Russian Federation could exploit uneven international capacity to identify and address CBW proliferation threats; lack of stringent know-your-customer and due-diligence practices for dual-use biological and chemical materials, equipment, and technology; and limited proliferation threat awareness by private sector and academic entities. In addition, proliferator states may leverage novel technologies, uneven oversight of commercial and research collaboration on dual-use topics, partners' habits of openness and data-sharing, and poor control of tacit knowledge to advance the Russian Government's proliferation activities.

To counter these threats, ISN/CTR seeks innovative approaches to mitigating Russia's evolving proliferation activities.

FY22 Partners for Foreign Capacity-Building Efforts: On the government side (ministries and agencies for science and technology, education, foreign affairs, law enforcement, finance/trade, health, transportation, and emergency management); in the private sector (financial institutions, logistics providers, manufacturers and distributors including pharmaceutical companies, research institutes, and educational institutions); and in the public sector (research institutes, educational institutes and nongovernmental organizations)

Program Objectives: ISN/CTR's foreign capacity building efforts seek to secure dual-use material, equipment, technology, knowledge, and expertise at partner government, commercial, or scientific institutions from illicit acquisition and exploitation for proliferation activities through the following activities:

- Providing open-source information that illuminates potential procurement, financial, and logistics networks supplying sensitive dual-use chemical and biological equipment, technology, dangerous pathogens, and/or weaponizable materials to the Russian Federation and its proxies for proliferation purposes and develop tailored, prompt, and actionable capacity-building activities;
- Enhancing partner public and private sector capacity and coordination to help prevent illicit procurement networks, supply chains, and transshipment that may wittingly or unwittingly facilitate CBW proliferation; and
- Providing awareness and best practices to networks, and communities of practice to protect expertise, research collaboration, explicit, and tacit knowledge from exploitation by the Russian Government for proliferation purposes.

Topics of interest: Virology, molecular biology, immunology, bacteriology, computational biology or chemistry, structural analysis, materials science, supply chain optimization, automation, and advanced manufacturing.

1. Open-Source Analysis to Identify Illicit CBW Facilitation Networks and Inform Capacity-Building: ISN/CTR will leverage open-source and commercially available data to identify actionable information on Russian Government-linked CBW proliferation-related activities. Projects will identify: a) procurement, financial, and logistics networks associated with proliferation-related supply chains; and b) research collaboration and peer-to-peer exchanges that have the potential to unwittingly facilitate dual-use knowledge and capabilities.

This open-source data should be tailored, prompt, and actionable — and will be shared with partner countries — to illuminate and expose obfuscated and illicit proliferation activities. Proposals will also develop cost-effective trainings for foreign partners, either remotely or in-person, to enhance partners' capacity to utilize open-source information to promote due diligence without long-term U.S. support. Projects will build or utilize existing commercial and collaborative networks to ensure the dissemination of analysis, datasets, and information. Typical open-source research projects should focus on the deep web (financial records, legal

records, commercial data sources), but can also be informed by the surface and dark web data sources.

Previous projects consisted of analytical reports, webinars, outreach campaigns via tailored social media, email educational campaigns, individual and institutional briefings, open-source capacity building and trainings, and industry screening platforms. These deliverables were derived from analysis of official public records, corporate filings, commercial trade data, and academic publications of entities that the U.S. Government believes to be associated with the Russian Federation's proliferation activities. ISN/CTR's FY22 efforts will:

- Identify illicit Russian Government, and Russian-linked, procurement, financial, and logistics networks and transactions that could facilitate CBW proliferation;
- Build or utilize existing commercial or collaborative networks to ensure broad dissemination of analysis, datasets, and other information;
- Leverage open-source and commercially available data to identify actionable information on Russian Government proliferation networks; and
- Develop cost-effective trainings to enhance partners' capacity to utilize open-source information to promote due diligence and enhance compliance.

Please note: This 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, this 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 capacity to meet their own open-source data needs to help address Russian Government proliferation activities.

Geographic Focus: Global, but country or region-specific 'deep dives' for financial, logistics, or supply hubs such projects will be considered.

2. **Securing Dual-Use Material, Equipment, and Technology:** ISN/CTR enhances partner capacities to identify and prevent Russian Government efforts to procure dual-use CBW materials, equipment, and technology. Projects will provide training, tabletop exercises, risk assessment methodologies, development and promulgation of best practices, and information sharing. Projects will build threat and risk-aware networks among regional governments, industry associations, financial institutions, biotechnology and pharmaceutical entities, and academic networks with commercial interests (e.g., supply chain related or when they involve procurement of dual-use materials, equipment, and technologies) and facilitate public-private partnerships to impede illicit acquisition of dual-use materials, equipment, and technology. ISN/CTR seeks creative, cost-effective engagements that leverage train-the-trainer, regional champions, and other self-led engagements by local partners. Projects may be bilateral or regional and include specific case studies or provide a targeted global engagement.

Previous projects included webinars, online courses, standard operating procedure development, and tabletop exercises engaging the biotechnology and chemical industries, financial and logistics networks, laboratory, and academic staff on Know Your Customer (KYC) and due diligence best practices, digital hygiene challenges, risk mitigation, strengthening public-private partnerships, and increasing list-based compliance with U.S. and international laws and norms. These trainings highlighted sites that the U.S. government believes to be associated with the Russian Government proliferation activities and highlight transactional activities with those sites. ISN/CTR's FY22 efforts will:

- Leverage open-source data to inform partner capacity building that enables them to identify and prevent engagement with Russian Government proliferation-linked supply chains;
- Provide training, tabletop exercises, threat and risk assessment methodologies, and information sharing to enable partners to develop due-diligence best practices;
- Build threat and risk-aware networks among inter-ministerial communities and regional governments that include a focus on cybersecurity in relation to preventing exploitation of the supply chain;
- Facilitate public-private partnerships that raise awareness and promulgate best practices that help to secure the supply chain and knowledge networks;
- Provide KYC and due diligence training for manufacturers, distributors, and shippers of sensitive dual-use materials, technology, and equipment that could be exploited by the Russian Government; and
- Facilitate regional exercises, roundtables, mentorships, and truly sustainable train-the-trainer activities that engage public and private sector partners.

Geographic Focus: Europe (Azerbaijan, Bulgaria, Estonia, Hungary, Latvia, Lithuania, Moldova, Poland, Romania, Slovakia, Slovenia, and Ukraine), East Asia and Pacific (Indonesia, Malaysia, Singapore, Taiwan, Vietnam), South and Central Asia (especially India), Africa (especially Guinea), and Western Hemisphere (especially Brazil).

- 3. Protection of Dual-Use Expertise and Tacit Knowledge from Exploitation:** ISN/CTR will support creative and cost-effective engagements that strengthen partner awareness of the links and risks associated with Russian Government proliferation activities and build self-sustaining information-sharing networks to promote due diligence among research institutes, academic communities, and other scientific and government stakeholders. This includes partnering with government, academic, and nongovernmental agencies to ensure they are not unwittingly engaging Russian Government, and Russian-linked, entities believed to be associated with WMD proliferation activities. Projects can be country-specific or regional case studies; bilateral, multilateral, or global projects; one sector or multisectoral approaches. Previous projects 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 dual-use research, knowledge, and funding from illicit exploitation; due-diligence; and KYC best-practices; and list-based compliance. Participants developed country-specific action plans to increase coordination and between traditional and non-traditional partners to support further dissemination of best-practices at the regional level. ISN/CTR's FY22 efforts will:

- Engage industry, academic, public, and private research institute partners to identify and promote cyber security best practices, policies, and procedures (and other sub-regulatory measures) and resources and promote their widespread adoption;
- Identify, promote, and implement practitioner-driven best practices to protect dual-use research collaborations, knowledge, and expertise from exploitation for proliferation purposes;
- Raise awareness of Russian Government proliferation threats, enable partners to identify potential ties with prohibited CBW-linked entities, and highlight the risks of doing business with them;
- Build networks among funders, universities, research institutes, industry, and non-traditional partners to counter proliferation threats; and
- Develop creative approaches for identifying and engaging non-traditional partners in awareness-raising, networking, and capacity building.

Geographic Focus: East Asia and Pacific (Indonesia, Malaysia, Singapore, Taiwan, Vietnam, Europe (Azerbaijan, Bulgaria, Estonia, Hungary, Latvia, Lithuania, Moldova, Poland, Romania, Slovakia, Slovenia, and Ukraine), South and Central Asia (especially India), Africa (especially Guinea), and Western Hemisphere (especially Brazil).

B. FEDERAL AWARD INFORMATION

Length of performance period: Twelve (12) Months

Award amounts: awards should range between \$250,000 to a maximum of \$500,000 per project

Total available funding: \$2,000,000

Type of Funding: FY21/22 Nonproliferation, Anti-Terrorism, Demining and Related Activities Funds under the Foreign Assistance Act.

Anticipated project start date: October 1, 2022

Funding Instrument Type: Cooperative agreement. Cooperative agreements are different from grants in that bureau staff are more actively involved in the grant implementation. The ISN/CTR office will play an active role in developing and shaping the materials developed and implanted during this award. ISN/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 (both domestic and international):

- Not-for-profit organizations
- Public and private educational institutions
- For-profit organizations

- Federally funded research and development centers
- Public International Organizations

2. Cost Sharing or Matching

This program does not require cost sharing, however proposals that demonstrate cost sharing will be welcomed.

The recipient is required to maintain written records to support all allowable costs that are claimed as its contribution to cost share, as well as costs to be paid by the Federal government. Such records are subject to audit. In the event the recipient does not meet the minimum amount of cost-sharing as stipulated in the recipient's budget, the Bureau's contribution may be reduced in proportion to the recipient's contribution.

3. Other Eligibility Requirements

To be eligible to receive an award, all organizations must have a unique entity identifier (Data Universal Numbering System/DUNS number from Dun & Bradstreet), as well as a valid registration on www.SAM.gov. Please see Section D.3 for information on how to obtain these registrations. Individuals are not required to have a unique entity identifier or be registered in SAM.gov.

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

D. APPLICATION AND SUBMISSION INFORMATION

1. Address to Request Application Package

Application forms required below are available at grants.gov

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.

2. 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 Times New Roman font, with a minimum of 1-inch margins.

The following documents are **required**:

Section 1 - Application for Federal Assistance (SF-424):

This form is part of the NOFO proposal package.

Section 2 – Project Proposal(s):

Using the provided template, the applicant must provide a completed project proposal. The proposal form must be completed in its entirety and clearly specify the proposed scope, deliverables, and timeline. Applicants must specify a point of contact for each project that is proposed.

Section 3 - Budget:

Also using the provided project proposal template, applicants must provide a budget for each project. The budget must identify the total amount of funding requested, with a breakdown of amounts to be spent in the following budget categories:

Application Submission Process: Applicants should submit project proposals electronically using Grants.gov. Thorough instructions on the Grants.gov application process is available at <http://www.grants.gov>. For questions relating to Grants.gov, please call the Grants.gov Contact Center at 1-800-518-4726.

3. Required Registrations:

Any applicant listed on the Excluded Parties List System (EPLS) in the System for Award Management (SAM) 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 listed on the EPLS can participate in any activities under an award. All applicants are strongly encouraged to review the EPLS in SAM to ensure that no ineligible entity is included.

All organizations applying for grants (except individuals) must obtain these registrations. All are free of charge:

- Unique entity identifier from Dun & Bradstreet (DUNS number)
- NCAGE/CAGE code
- www.SAM.gov registration

Step 1: Apply for a DUNS number and an NCAGE number (these can be completed simultaneously)

DUNS application: Organizations must have a Data Universal Numbering System (DUNS) number from Dun & Bradstreet. If your organization does not have one already, you may obtain one by calling 1-866-705-5711 or visiting <http://fedgov.dnb.com/webform>

NCAGE application: Application page here:

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

Instructions for the NCAGE application process:

<https://eportal.nspa.nato.int/AC135Public/Docs/US%20Instructions%20for%20NSPA%20NCAGE.pdf>

For NCAGE help from within the U.S., call 1-888-227-2423
For NCAGE help from outside the U.S., call 1-269-961-7766
Email NCAGE@dliis.dla.mil for any problems in getting an NCAGE code.
Step 2: After receiving the NCAGE Code, proceed to register in SAM.gov by logging onto:
<https://www.sam.gov>. SAM registration must be renewed annually. Please note that your CCR registration must be annually renewed.

4. Submission Dates and Times

Applications must be submitted on or before January 31, 2022, 11:59 p.m. Eastern time. Applications submitted after 11:59 p.m. will be ineligible for consideration. Begin the application process early, as this will allow time to address any technical difficulties that may arise in advance of the deadline. There will be no exceptions to this application deadline.

5. Funding Restrictions

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

6. Other Submission Requirements

All application materials must be submitted electronically through www.Grants.gov.

E. APPLICATION REVIEW INFORMATION

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 including approaches to participant recruitment.

- **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 training period, and describe observable progress in the adoption, implementation, or enhancement of nonproliferation or sanctions enforcement and compliance best practices
- **Diversity and Inclusion:** 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 CTR's diversity, equity, inclusion, and accessibility (DEIA) objectives through their programming. Submitted plans will be evaluated separate to the overall evaluation of projects, to ensure that submissions with DEIA plans will not result in the higher evaluation of any proposal package over one that did not submit a DEIA plan.
- **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. 4 or later), System and Information Integrity Policy (SI-1) as follows:
 1. Identification and Authentication: Implement multifactor authentication for network access and local access.
 2. Access Controls: Implement security controls for information sharing, remote access and wireless access including:
 - a. Monitoring, controlling, and protecting remote and wireless access to information by auditing information systems components (e.g., workstations, notebook computers, smartphones, and tablets).
 3. Incident Handling: Monitor and report 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.

F. FEDERAL AWARD ADMINISTRATION INFORMATION

1. Federal Award Notices

The 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 project 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.

Anticipated Time to Award: Applicants should expect to be notified of the *recommended* concepts within 90 days after the submission deadline. Following this initial notification, **selected applicants will be expected to submit a full application within 30 days.** ISN/CTR staff will provide information at the point of notification about the requirements for the full application, which may include revisions to the activities. The full applications will not be subject to further competition, but must incorporate any suggested changes made by ISN/CTR. Issuance of this NOFO does not constitute an award commitment on the part of the Government, nor does it commit the Government to pay for costs incurred in the preparation and submission of proposals. Further, the Government reserves the right to reject any or all proposals received.

Project Implementation Meeting: The recipient should expect to have a pre-project implementation meeting with ISN/CTR within thirty days after the cooperative agreement is awarded and before any work is performed for the award.

2. Administrative and National Policy Requirements

Terms and Conditions: Before applying, applicants should review all the terms and conditions and required certifications that will apply to this award, to ensure that they will be able to comply. These include: 2 CFR 200, 2 CFR 600, Certifications and Assurances, and the Department of State Standard Terms and Conditions.

3. Reporting

Reporting Requirements: As a cooperative agreement, reporting and deliverable requirements for this project exceed those of typical grants. Applicants should pay special attention to these enhanced reporting and deliverable requirements. Specifically:
Using a template provided by ISN/CTR, the Recipient shall submit quarterly progress reports to the designated Grants Officer Representative (GOR), program distribution list, and to the following email address ISN-CTR-BUDGET@state.gov detailing:

- Assistance activities conducted during the reporting period;

- Milestones and successes achieved to date;
- Key assistance activities remaining to be implemented with a projected timetable;
- Details of any problems encountered with proposed solutions; and
- Any other pertinent information requested by ISN/CTR.
- The Recipient shall provide the GOR with copies of all materials developed under this cooperative agreement.
- In addition to regular quarterly reports, the Recipient shall furnish the GOR with ad hoc reports as requested from time to time.
- In addition to the above, the Recipient shall submit quarterly financial reports throughout the project period. Financial reports are due 30 days after the reporting period. Final programmatic and financial reports are due 90 days after the close of the project period

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

If you have any programmatic questions about the grant application process, please contact:
CTRSpecialProjectsProposals@state.gov

For interagency agreement (IAA) submissions, directly submit application to the relevant program team and copy the budget team (ISN-CTR-BUDGET@state.gov).

Direct any NOFO submission (non-programmatic) questions to:
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.

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

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 the 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.