U.S. DEPARTMENT OF STATE
U.S. EMBASSY MAJURO
Notice of Funding Opportunity (NOFO)

Announcement Type:	New Announcement
Assistance Type:	Cooperative Agreement
Funding Opportunity Title:	Republic of the Marshall Islands (RMI) Cybersecurity Capacity Building
Funding Opportunity Number:	DOS-MHL-FY21-001
Catalog of Federal Domestic Assistance (CFDA) Number:	19.124
Total Available Funding:	$500,000
NOFO Issuance Date:	May 6, 2021
Deadline for Receipt of Questions:	June 18, 2021 at 5:00PM Eastern Daylight Time
Application Deadline:	July 6, 2021 at 11:59PM Eastern Daylight Time
Eligibility Category:	U.S. Non-profit/non-governmental organizations NGOs) having a 501(c)(3) status with the IRS, or overseas-based non-profit/non-governmental organizations, and U.S. and overseas private/state institutions of higher education (See full eligibility criteria below in Section C).

Executive Summary:

The U.S. Department of State (DOS), U.S. Embassy Majuro announces this Notice of Funding Opportunity ("NOFO") for Republic of the Marshall Islands (RMI) Cybersecurity Capacity Building.

A cooperative agreement for up to $500,000 U.S. Dollars (USD) in FY 2020 Economic Support Funds (ESF) will be awarded (pending availability of funds) for work that will support the Republic of the Marshall Islands' (RMI) aspiration to establish the ability to secure its Information and Communications Technology (ICT) from illegal and malicious intrusion by 1) developing an effective, Government-wide regulatory framework; 2) developing a cyber-ready workforce; and 3) by demonstrating effective cybersecurity systems and procedures for one or more select services. The period of performance is two years. Funding authority rests in the Foreign Assistance Act of 1961, as amended.

Contact Person: See Section G.

Please read carefully the entire solicitation package if you plan to submit an application; there are steps that you should take immediately in order to make your submissions by the deadline.

A. PROJECT DESCRIPTION

A.1. Background

The Republic of the Marshall Islands (*RMI*) does not have a national cybersecurity strategy, although with assistance from the Department of State, the Ministry of Transportation, Communication and Information Technology has recently initiated a project to establish a cybersecurity strategy. RMI presently lacks a dedicated cybersecurity office, a trusted corporate-wide network, and overarching cybersecurity policies and procedures that apply to all RMI public infrastructure and ICT. Government officials use personal email accounts to conduct public business. Sharing of sensitive information with the RMI by international entities is hampered by the reluctance of these entities to communicate via the RMI's insecure IT systems. Critical communication and electrical infrastructure lack sufficient protection against cyber intrusion. Cyber awareness among RMI Government ministries is in general low.

The RMI is at high risk for malicious, illegal and damaging intrusions to its ICT. The RMI lacks Government-wide policies and procedures that protects critical infrastructure and ICT from cybersecurity intrusion and malicious use. There is no system currently in place that prevents the purchase of ICT equipment and software from untrusted vendors. The RMI does not have a cybersecurity governance and reporting framework, physical access controls, cybersecurity certification of Government employees and new employee training. The various RMI ministries do not routinely use malware protection, virus checking, and/or virtual boot-up software. The Government lacks policies with respect to downloading of applications on Government ICT, use

RMI has some legislative offences relating to cybercrime and child protection matters. However, capacity for enforcing cybercrime offences is low. A Computer Crimes Bill was developed in 2011 but this has not progressed.

A2. Program Goals

This project will enable the RMI Government to detect and prevent malicious cyber incidents to its ICT and critical infrastructure, protect sensitive data, and provide secure and safe egov services to its citizens.

Objective 1: The RMI Government will develop a "cyber-ready" workforce in which its employees have been effectively trained in cyber security procedures and practices.

Objective 2: RMI will have issued Government-wide cyber security standards that effectively secures its ICT, to include such items as access controls, authentication, Personally Identifiable Information (PII), data backup, encryption, use of virus checking software and firewalls, use of removable media, purchase of ICT from trusted sources, patch and update maintenance, downloading of applications, industrial controls, software access, privilege, and admin permissions, account deactivation upon employee separation, record storage and disposition, and cyber incident response.

Objective 3: One or more RMI Government records (e.g., health records) or services (e.g., email) will be demonstrably more cybersecure.

A3. Expected Results

Specific results could include the following:

Result 1: RMI Government Ministries will be able to exchange sensitive information with its partners without restriction due to perceived RMI cybersecurity deficiencies.

Result 2: RMI will be able to demonstrate that its uniform, Government-wide cybersecurity standards and practices conform to international best practices.

Result 3: RMI will be able to demonstrate that it has successfully detected and prevented several malicious cybersecurity incidents.

Results 4: RMI citizens will express confidence that RMI egov services will protect their sensitive data.

A4. Main Activities

To achieve the goals and expected results, the program could include the following:

Activity 1: Cybersecurity Improvements for Select Records and/or Services

Activity 2: Development of Cybersecurity Standards

Activity 3: Cyber Ready Workforce - Cybersecurity Training

Each of these activities is explained below.

Cybersecurity improvements for select services and systems. Offerors should propose to provide training, advice, mentoring, procedure and policy development, and technical advice about one or two specific RMI Government services that result in demonstrable, concrete improvement in cybersecurity for those services.

Offerors should prioritize services for which cybersecurity improvements can be attained by the RMI at modest expense in a relatively short timeframe (e.g., purchase of anti-virus software, development of policies and procedures for downloading of software, implementation of physical access controls, development of policies and training related to protection of Personal Identifiable Information (PII)).

Examples of possible services include email services, medical records, judicial records, birth records, tax and social security records, and other RMI Government-maintained records with sensitive data or which include PII. Other examples include advice and assistance to the RMI Government that leads to the installation and maintenance of standard virus-checking software on all government computers, or developing policies and procedures related to physical access control to ICT systems, and certification and control of software applications on RMI ICT. Example of systems include the local area network (LAN) used by the Ministry of Finance for the government-wide financial management system and the system used by the National Telecommunications Authority (NTA) to operate RMI communications infrastructure.

Offerors are encouraged to propose activities that will ensure that success in improving cybersecurity for one or more RMI Government services or systems can be leveraged to promote and achieve similar success on a broader scale and that the experience with one or more services and systems will inform the development of a Government-wide regulatory framework. Offerors should present strategies for socializing successes with the selected service(s) in order to build momentum for broader RMI cybersecurity improvements.

Cybersecurity Regulatory Framework for Infrastructure and ICT. Assist the RMI to develop and deploy Government-wide policies and procedures that protect critical RMI infrastructure and ICT from cybersecurity intrusion and malicious use. A regulatory framework might cover the purchase of ICT equipment and software from trusted vendors or identifying prohibited sources; cybersecurity governance and reporting; physical access controls; cybersecurity certification of Government employees and new employee training; use of malware protection, virus checking, and/or virtual boot-up software; and policies with respect to downloading of applications on Government ICT, use of removable media, multi-factor authentication policies for system access, patch and update maintenance, data backup, protection of PII, encryption, software access, privilege, and admin permissions, account deactivation upon employee separation, record storage and disposition, and cyber incident response.

While the RMI currently lacks a cybersecurity governance framework, recipient will be expected to work closely with the RMI Government leadership and counterparts, especially those in the Ministry of Transportation & Communications, the Office of the Attorney General, and the Office of Auditor General on this component of the project. Offerors are encouraged to propose innovative approaches for issuance of and monitoring compliance with Government-wide cybersecurity standards in the absence of a dedicated RMI cybersecurity office that has the requisite enforcement authorities. Examples of such approaches might include phased introduction of regulations, decentralized compliance monitoring, gradual and/or voluntary migration paths for compliance, “champions”

within individual ministries, dissemination of local examples of the effects of cyber-security intrusions, cyber security "challenges", and special recognition of early adopters.

Offerors should include a strategy for ensuring that cybersecurity standards are consistent with other donor projects, especially the World Bank's RMI Digital project.

Cyber-Ready Workforce - Certification Training Program. Develop curricula, standards, and education and training approach for an RMI cybersecurity certification program that contributes to a cyber-ready workforce. Offerors are encouraged to propose utilization of a Training-of-Trainers (ToT) approach so that the RMI Government will be able to independently deliver the basic level certification course on a continuing basis for all employees whose work requires the use of Government-owned ICT equipment and software.

Offerors should present a strategy for ensuring that their proposed education and training approach, curriculum, materials, and instruction methods are tested and effective in promoting a cyber-ready workforce.

The successful recipient will be expected to engage with the RMI Government and local business community in the development of its curriculum to ensure that recipients of the training gain the skills they need for basic cybersecurity awareness and skills.

To the extent possible, training should rely on training and educational institutions, resources, and projects which already exist within the Marshall Islands and/or the Pacific region. These include the Public Service Commission of the Government of the Marshall Islands, College of the Marshall Islands (CMI), the University of the South Pacific (USP), PaCSON, PICISOC, and CyberSafety Pasifika. Offerors are encouraged to propose the incorporation of virtual and on-line training modules into their cyber-security curriculum, especially those available at no or low cost (e.g., training modules available from the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and the Cyber-Ready Institute).

A5. Performance Indicators

The project should monitor and report on performance indicators that are specific, measurable, achievable, reasonable, and time-bound. Establish, where possible, performance baseline data and expected performance targets for each expected result, and include details on what sources of data will be used to document performance, how the indicators will be measured, frequency of measurement, and units of measure. Where possible, indicators should also allow for sex disaggregation. Indicators should reflect key project outputs or outcomes that reflect on the primary goals or objectives of the project and that the implementer can collect with high quality data.

Applicants must fill out the table below and insert it into the proposal document. Additional non-Department of State (DOS) indicators may be added that are relevant to the project by adding rows to the chart.

All applicable indicators should be included in the proposal and subsequent to the award, routine, periodic reporting of all indicators will be required. The implementer will be responsible for quarterly progress reporting on each performance indicator included in the award agreement as well as analysis of progress or impediments to reach indicator targets.

The following are required indicators. Applicants are welcome to propose other indicators relevant to the primary objectives and expected results of the project.

	Outcome Indicators	***Targets***
Output 1.	Number of cybersecurity curricula developed and tested	1
Output 2.	Number of RMI employees successfully certified as "cyber-ready"	50
Output 3.	Number of records or systems with at least 10 documented improvements in their levels of protection from cyber security intrusion	2
Output 4.	Number of cybersecurity policy areas for which RMI has promulgated a Government-wide standard (example of an policy area: Downloading of apps onto Government ICT)	12

A6. Substantial Involvement

U.S. Embassy Majuro anticipates awarding a cooperative agreement as a result of this NOFO. The distinction between grants and cooperative agreements revolves around the existence of "substantial involvement." Cooperative agreements require greater involvement from the Federal government during the implementation of the award agreement. For this cooperative agreement, it is anticipated that the Department of State will be substantially involved in the following areas at a minimum:

1. Approval of one stage of work before the next stage can begin;
2. Approval of cybersecurity training curriculum
3. Selection of records and/or services targeted for cybersecurity improvement
4. Involvement in the selection of participants or program venues;
5. Joint preparation of presentation of project results with the recipient;
6. Coordination with other cooperating agencies or U.S. embassies (if applicable)

B. FEDERAL AWARD INFORMATION

U.S. Embassy Majuro anticipates having approximately $ 500,000 of FY 2020 Economic Support Funds (ESF) available to support one successful application submitted in response to this NOFO, subject to the ability of funding. The authority for this funding opportunity is found in the Foreign Assistance Act of 1961, as amended (FAA).

Applicants should include an anticipated start date between August and September 2021 and the period of performance should be two years.

The Department of State may make award(s) on the basis of 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 Department of State reserves the right (though it is not under obligation to do so), however, to enter into 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.

Depending on the quality of performance and other factors, U.S. Embassy Majuro may consider additional supplemental funding to continue activities and extend the period of performance, if funds are available and the Embassy and the Recipient mutually agree.

Summary of Award Information

Type of Award	Cooperative Agreement
Type of Funding	FY2020 Economic Support Funds (ESF)
Funding Amount:	$500,000
Number of Awards:	1
Award Date:	August-September 2021
Project Completion Date:	September 2023

This notice is subject to availability of funding.

C. ELIGIBILITY INFORMATION

C.1 Eligible Applicants

U.S. Embassy Majuro welcomes applications from U.S. Non-profit/non-governmental organizations (NGOs) having a 501(c)(3) status with the IRS, or overseas-based non-profit/non-governmental organizations, and U.S. and overseas private/state institutions of higher education

For-profit and commercial firms are not eligible to apply in response to this NOFO.

Please see 2 CFR 200.307 for regulations regarding program income.

C.2 Cost Sharing or Matching

Providing cost sharing, matching, or cost participation is not an eligibility requirement for this NOFO.

Please note: If cost-share is included in the budget then the recipient must 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 Department of State's contribution may be reduced in proportion to the recipient's contribution.

C.3 Other Eligibility Requirements

In order 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.

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

Organizations may only submit one application per organization. If more than one application is submitted by an organization, only the first application received from that institution will be reviewed for eligibility and funding.

D. APPLICATION AND SUBMISSION INFORMATION

D.1 Address to Request Application Package

Applicants can find application forms and other materials need to apply on Grants.gov and under the announcement title and funding opportunity number provided above.

Note: Applications will not be accepted through grants.gov.

Please contact the point of contact listed in section G if requesting reasonable accommodations for persons with disabilities or for security reasons. Please note: reasonable accommodations do not include deadline extensions.

Please read carefully the entire announcement and follow the guidelines below before sending inquiries or submitting proposals.

D.2 Content and Form of Application Submission

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

For all submitted application documents, please ensure:

- The proposal clearly addresses the goals and objectives of this funding opportunity
- All documents are in English. If an original document within the application is in another language, an English translation must be provided (please note: the Department of State, as indicated in 2 CFR 200.111, requires that English is the official language of all award documents. If any documents are provided in both English and a foreign language, the English language version is the controlling version);
- All budget costs are in U.S. dollars;
- All pages are numbered, including budgets and attachments;
- All documents are formatted to 8 ½ x 11 paper; and,
- All documents are single-spaced, 12-point Times New Roman font, with 1-inch margins. Captions and footnotes may be 10-point Times New Roman font. Font sizes in charts and tables, including the budget, can be reformatted to fit within 1-page width.

Complete applications must include the following required documents:

1. Completed and signed **SF-424**, **SF-424A**, and **SF-424B** and **SF-LLL** forms. These forms are available electronically via Grants.gov. *The SF-424 B is required only for those applicants who have not registered in SAM.gov or recertified their registration in SAM.gov since February 2, 2019 and completed the online representations and certifications. The SF-LLL is required for applicants that may engage in lobbying activities.*

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. **Table of Contents** that includes a page numbered contents page and any attachments.

4. **Proposal Narrative** (not to exceed 10 pages), should be organized using the following section headings: Executive Summary, Organizational Capacity and Past Performance, Program Strategy, Performance Monitoring and Evaluation, and Management Plan. Please see the "Narrative Components" section below for details on the information to include in the proposal.
   (The 10-page limit does not include the Summary Page, Table of Contents, Budget, Budget Narrative, Letter of Disclosure, Letter of Institutional Support, NICRA, Audit, CVs, or SF-424s).

5. **Summary and Detailed Line-Item Budget** (in Microsoft Excel) that includes three [3] columns including the request to U.S. Embassy Majuro, any cost sharing contribution, and total budget (see below for more information on budget format). **The federal share**

requested should not exceed the amount of funds available under section B. A summary budget should also be included using the OMB approved budget categories (see SF-424A for budget categories). Costs must be in U.S. dollars. Detailed line-item budgets for sub-awardees should be included in additional tabs within the excel workbook. A template budget is provided, but is not required, as long as the submitted budget follows OMB budget categories.

6. **Budget Narrative** (in Microsoft Word) that includes substantive explanations and justifications for each line item in the detailed budget spreadsheet, as well as the source and a description of all cost-share offered. For ease of review, we recommend applicants order the budget narrative as presented in the detailed budget. Personnel costs must include a clarification of the roles and responsibilities of all staff, base salary, and percentage of time devoted to the project. The budget narrative should support the activities described in the proposal and provide additional information that might not be readily apparent in the detailed-line item budget, not simply repeat what is represented numerically in the budget, i.e. salaries are for salaries or travel is for travel. The budget narrative should also explain any cost share provided.

7. **NICRA**: If your organization has a Negotiated Indirect Cost Rate Agreement (NICRA) and includes NICRA charges in the budget, your most recent NICRA should be included as a PDF file. This document will not be reviewed by the panelists, but rather used by project and grant staff if the submission is recommended for funding and therefore does not count against the submission page limitations. If your proposal involves subawards to organizations charging indirect costs, please submit the applicable NICRA.
Per 2 CFR200.414(f), organizations that have never had a NICRA may request a de minimis indirect rate of up to 10% of the Modified Total Direct Costs (MTDC) as defined in 2 CFR 200.68. *MTDC excludes equipment, capital expenditures, charges for patient care, rental costs, tuition remission, scholarships and fellowships, participant support costs and the portion of each subaward in excess of $25,000*. The budget narrative should indicate what costs will be covered using the 10% de minimis rate.

8. **Letter of Disclosure** for proposed consultants/personnel (if applicable) of potential conflicts of interest, employment with a local/state/federal government.

9. A PDF file copy of your organization's most recent **single audit** is required, if your organization meets the threshold as defined in 2 CFR 200 Subpart F.

Narrative Components
As stated above, the proposal may be a maximum of 10 pages. The proposal must include the following information:

a. Executive Summary
This section should be a succinct one-page summary containing information that the applicant believes best represents its proposed program and includes: the name and contact information for the project's main point of contact; the project's purpose; targeted countries; program length (dates/duration); total funding requested (indicate any sub-grants proposed); project's goals,

primary objectives and expected results (highlighting any aspects of innovation, sustainability and impact of the project); involvement or use of any NGO's or civil society organizations; and expected results and sustainability; and a one-paragraph program description. Countries of implementation are those countries or participants from countries that will receive financial or technical support as a result of this project.

b. Organizational Capacity and Past Performance

This section of the application provides information about the applicant organization. It provides evidence that the applicant has the ability to successfully carry out the program activities of the agreement.

- Provide a description of the applicant organization – including its general purpose, goals, annual budget (including funding sources), and major past and current activities and projects undertaken.
- Discuss the applicant's experience on developing and implementing cybersecurity capacity building programs.
- As an attachment (which does not count as part of the 10 pages), please provide at least one past performance reference which describes any contracts, grants, cooperative agreements which the applicant organization has implemented involving similar or related programs over the past three years. Please provide the reference in an attachment and include the following information: name and address of the organization for which the work was performed; current telephone number and email address of responsible representative from the organization for which the work was performed; contract/grant name and number (if any), annual amount received for each of the last three years and beginning and end dates; brief description of the project/assistance activity and key project accomplishments/results achieved to date.

c. Program Strategy

- Propose a clear and realistic implementation plan to significantly address the Program Goals in Section A2.
- The proposal should further outline the expected and achievable results for the project which should include suggestions in Section A3. It should also outline the relevant and appropriate Main Activities to accomplish the goals and expected results, which could include those found in Section A4. Explain the assumptions on which the success of the project depends, and the involvement of other stakeholders.
- In table format, please present a brief, one- to two-page work plan matrix (which does count as part of the 10 pages), with a timeline including target dates for activities for the life of the agreement, which reflects the overall program approach, and objectives. The following timeline below is provided as an example.

Primary Activities, Deliverables, and/or Milestones	Q1	Q2	Q3	Q4	Q5	Etc.
Project Monitoring Plan	X					

XYZ Activity	X	X	X	X		
Activity 123			X	X	X	
Etc.						

d. Performance Monitoring and Evaluation Plan

- Discuss how progress towards the expected results will be measured, as outlined by the Performance Indicators in Section A5. Identify which performance indicators will be measured and how data on these indicators will be collected, analyzed, and used for program management. Present indicators linked to specific project objectives in table format and include source of data and proposed frequency of collection. See the full list of Performance Indicators in Section A5.

e. Management Plan

- Describe the proposed management structure for this project and provide a project organizational chart in the attachments. Include in the narrative a description of the responsibilities of all principal organizations and staff involved, reporting relationships, authority and lines of communication within and between each of these organizations.
- Include job descriptions and CVs of key staff (Project Director, etc.) as attachments (do not count as part of the 10-page limit), which demonstrate that the proposed key staff are consistent with the requirements and needs of the project. The project should have a designated Project Director who will be expected to have lead responsibility for communicating with the Department of State. Note the location where key staff will be based.
- Recognizing that COVID-19 has limited where and when staff/participants can travel, the Recipient should also include a contingency plan should restricted travel remain through some portion of the period of performance. Contingency plans could include remote or virtual training tools.

Note: Applications that do not include all required documents will be marked as incomplete, and will therefore be deemed technically ineligible.

U.S. Embassy Majuro retains the right to ask for additional documents not included in this NOFO. Additionally, to ensure all applications receive a balanced evaluation, the Grants Review Panel will review the first page of the requested section up to the page limit and no further. U.S. Embassy Majuro encourages organizations to use the given space effectively.

D.3 Unique Entity Identifier and System for Award Management (SAM)

All organizations applying for grants 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@dlis.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.

Applicants must have an active registration in SAM (www.sam.gov) prior to submitting an application, must prove a valid Unique Entity Identifier (UEI) number, formerly referred to as a DUNS number, and must continue to maintain an active SAM.gov registration with current information at all times during which it has an active Federal award or an application or plan under consideration by the U.S. government. **If an organization does not have an active registration in SAM.gov prior to submitting an application, the application will be deemed ineligible.** Note: The process of obtaining a SAM.gov registration may take anywhere from 4-8 weeks. Please begin your registration as early as possible.

The Unique Entity Identifier (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. SAM is the Federal government's primary database for complying with FFATA reporting requirements. OMB designated SAM as the central repository to facilitate applicant and recipient use of a single public website that consolidates data on all federal financial assistance. Under the law, it is mandatory to obtain a UEI number and register in SAM.

SAM 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 and to also maintain its active registration in SAM.

An exemption from this requirement may be permitted on a case-by-case basis if the applicant's identity must be protected due to possible endangerment of their mission, their organization's status, their employees, or individuals being served by the applicant. Organizations requesting an exemption should email the point of contact listed in Section G of this NOFO.

Please note: foreign organizations will be required to register with the NATO Support Agency (NSPA) to receive a NATO Commercial and Government Entity (NCAGE) code in order to register in SAM. NSPA will forward your registration request to the applicable National Codification Bureau (NCB) if your organization is located in a NATO or Tier 2 Sponsored Non-NATO Nation. (As of January 2015, NATO nations included Albania, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Turkey, United Kingdom, and the United States of America; and Tier 2 nations included Australia, Austria, Brazil, Finland, Israel, Republic of Korea, Malaysia, Morocco, New Zealand, Serbia, and Singapore.)

NSPA and/or the appropriate NCB forwards all NCAGE code information to all Allied Committee 135 (AC/135) nations, which as of January 2015 also included Afghanistan, Argentina, Bosnia & Herzegovina, Brunei Darussalam, Chile, Colombia, Egypt, Georgia, India, Indonesia, Japan, Jordan, Montenegro, Oman, Papua New Guinea, Peru, Saudi Arabia, South Africa, Sweden, Thailand, Republic of Macedonia, Ukraine, and the United Arab Emirates.

D.4 Submission Dates and Times

Applications are due no later than 11:59 p.m. Eastern Daylight Time (EDT), on July 6, 2021

Applicants are urged to begin the application process well before the submission deadline. No exceptions will be made for organizations that have not completed the necessary steps.

Applications received after the deadline will not be considered.

Grants.gov automatically logs 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.

If ultimately provided with a notification of intent to make a Federal award, applicants typically have two to three weeks to provide additional information and documents requested in the notification of intent. The deadlines may vary in each notification of intent and applicants must adhere to the stated deadline in the notification of intent.

D.5 Funding Restrictions

The Department of State will not consider applications that reflect any type of support for any member, affiliate, or representative of a designated terrorist organization. No entity listed on the Excluded Parties List System in SAM is eligible for any assistance.

Project activities that provide training or other assistance to foreign militaries or paramilitary groups or individuals will not be considered for 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) (2015), "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. Federal awards generally will not allow reimbursement of pre-award costs; however, the Grants Officer may approve pre-award costs on a case-by-case basis. Generally, construction costs are not allowed.

D.6 Other Submission Requirements

All application submissions must be made electronically via Grants.gov. This system requires registration by the applying organization.

It is the responsibility of the applicant to ensure that it has an active registration in Grants.gov and that an application has been received by Grants.gov in its entirety. U.S. Embassy Majuro bears no responsibility for disqualification that result from applicants not being registered before the due date or for data errors resulting from transmission or conversion processes. Additionally, you must 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 solicitation and these instructions.

Should an applicant experience technical issues, contacted the helpdesk, and is not receiving timely assistance (e.g. if you have not received a response after 2 days of contacting the helpdesk), you may contact the point of contact listed in section G, who may assist in contacting the appropriate helpdesk. Applicants should document their efforts in contacting the helpdesk.

E. APPLICATION REVIEW INFORMATION

E.1 Criteria

Each application will be evaluated and scored on the five-part Proposal Components and the two-part Budget Components using a 100-point scale. Each application will be evaluated individually against the criteria below and not against competing applications.

Proposal Narrative: The Review Panel will score each of the five sections of the Proposal Narrative based on how completely they address the bulleted points described in the Proposal Narrative Guidance in Section D2. The Panel will assign up to 80 points for the proposal narrative. The importance of each section is indicated by the maximum score as follows:

- Executive Summary – 10 points
- Organization Capacity and Past Performance – 20 points
- Program Strategy – 25 points
- Performance Monitoring and Evaluation – 15 points
- Management Plan – 10 points

Budget: The Review Panel will also review the budget components in order to assign up to 20 points for the overall program budget and cost-effectiveness. Proposals should keep estimated overhead and administrative costs as low as possible and have proposed expenditures that are reasonable, allowable, and allocable to the proposed project activities and reflect the applicant's understanding of the allowable cost principles established by Office of Management and Budget (OMB) in 2 CFR 200. Applicants should provide clear explanations and justifications for costs in relation to the work involved. All budget items should be clearly explained and justified to demonstrate its necessity, appropriateness, and its link to the project objectives. Amount of funding contributed by the applicant, sub-awardees, and other partners – while not required – shows a commitment to the success of the project.

- Budget Appropriateness – 10 points
- Cost-effectiveness – 10 points

E.2 Review and Selection Process

Each application will receive a balanced evaluation by the Grants Review Panel. All technically eligible applications for a given notice of funding opportunity are reviewed against the same criteria, listed above. Additionally, the Grants Review Panel will evaluate how the application addresses the NOFO request, U.S. foreign policy goals, and the priority needs of U.S. Embassy Majuro overall.

The Grants Review Panel generally includes representatives from the Department of State, and may include additional panelists from other U.S. embassies and/or other U.S. government departments or agencies. All Panelists must sign non-disclosure agreements and conflicts of interest agreements.

The Grants Review Panels 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. To ensure effective use of funds, conditions or recommendations may include requests to increase, decrease, clarify, and/or justify costs and project activities.

E.3 Federal Awardee Performance & Integrity Information System

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 (currently FAPIIS) (see 41 U.S.C. 2313).

The applicant, at its option, may review information in the designated integrity and performance systems accessible through SAM and comment on any information about itself that a Federal awarding agency previously entered and is currently in the designated integrity and performance system accessible through SAM.

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.

F. FEDERAL AWARD ADMINISTRATION INFORMATION

F.1 Federal Award Notices

The Department of State will provide a separate notification to applicants on the result of their applications. Successful applicants will be notified by email. 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 panel's conditions and recommendations, Congressional Notification requirements being met, and final review and approval by the Department's warranted Grants Officer.

The grant award or cooperative agreement will be written, signed, awarded, and administered by the warranted Grants Officer. The signed assistance award agreement is the sole authorizing document and it will be provided electronically to the recipient's authorized signatory for review and signature via email. The recipient may only start incurring program expenses beginning on the start date show on the 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 as the discretion of the Department of State.

F.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
- 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:

- President's September 2, 2020 memorandum, entitled *Memorandum on Reviewing Funding to State and Local Government Recipients of Federal Funds that Are Permitting Anarchy, Violence, and Destruction in American Cities*;
- *Executive Order on Protecting American Monuments, Memorials, and Statues and Combating Recent Criminal Violence* (E.O. 13933); and
- 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).

Applicants should plan to coordinate with the Department of State throughout the course of the agreement to ensure assistance is provided only to eligible participants.

F.3 Reporting

Recipients will be required to complete regular financial reports and program progress reports. The award document will specific how often these reports must be submitted, but will be as frequently as quarterly. Please note that all substantiating documentation supporting reporting and data collected, including survey responses and contact information, must be maintained for a minimum of three years and provided to the Department of State upon request. All reports must be written in English

1. **Financial Reports**: The recipient will be required to submit quarterly financial reports through the project period. The Federal Financial Report (FFR SF-425) is the required form for the financial reports. Form FFR (SF-425) can be found here: https://www.grants.gov/web/grants/forms/post-award-reporting-forms.html#sortby=1 Financial reports are due 30 calendar days after the end of each reporting period.

   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.

2. **Progress Reports:** The recipient will be required to submit quarterly narrative progress reports. Progress reports are due 30 days after the end of the reporting period. Where relevant, progress reports should include the following information:

   - Significant activities of the period and how activities reflect progress toward achieving goals;
   - Evaluation of progress on goals/objectives with quantitative and qualitative data, as appropriate;
   - Any problems/challenges in implementing the project and a corrective action plan;
   - Evaluation of accomplishments with quantifiable information on goals and objectives to date as available, including reporting on agreed-upon indicators;

- An update on expenditures during the reporting period; and
- Supporting documentation or products related to project activities (such as surveys, travel, etc.).
- Performance indicator results and supporting documentation
- Project Spotlight highlighting a significant area of progress under the agreement as well as photos of implementation

Quarterly progress reports should also reflect the awardee's continued focus on measuring the project's impact on the overarching goals or problems the project set out to address. An assessment of the overall project impact, as appropriate, should be included in each quarterly project report.

3. **Final Report:** A final narrative report and financial report will be required within 120 days after the completion of the award. The final narrative should include an in-depth impact assessment and/or project evaluation. More 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.

The Department of State reserves the right to request any additional programmatic and/or financial project information during the award period of performance.

G. CONTACT INFORMATION

Any prospective applicant who has questions concerning the contents of this NOFO should email them to Jeremiah Knight (KnightJA@state.gov) with the subject "[Applicant Name] RMI Cybersecurity Capacity Building." To maintain fairness and transparency in competition, U.S. Embassy Majuro 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 June 18, 2021. U.S. Embassy Majuro will periodically create a document of submitted questions with answers and upload it to the announcement page in grants.gov. Prospective applicants are advised to review the announcement page in grants.gov for any updates. Note that once the NOFO deadline has passed, DOS staff in Washington, D.C. and overseas and U.S. Embassies/Missions may not discuss this completion with applicants until the review process has been completed.

With the exception of technical submission questions, during the solicitation period U.S. Department of State staff in Washington and overseas shall not discuss this competition with applicants until the entire proposal review process has been completed and an award has been made.

H. OTHER INFORMATION

H1. Monitoring Site Visits

Department of State may conduct a monitoring site visit during the lifetime of a grant. The site visit allows the Department's grant management personnel to gather additional information on the recipient's ability to properly implement the project, manage Department of State funds, and substantiating document for programmatic, indicator, and financial reporting. The site visit may involve the review of the programmatic progress (progress on activities, sub-recipient/consultant work, data quality, etc.) as well as administrative and financial management and controls.

H.2 Disclosures

The Department of State 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 the 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 Department of State representative. Explanatory information provided by the Department of State that contradicts this language will not be binding. Issuance of the NOFO and negotiation of applications does not constitute an award commitment on the part of the U.S. government. The Department reserves the right to reduce, revise, or increase proposal budgets in accordance with the needs of the project evaluation requirements.

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. The. U.S. government reserves the right to reject any or all proposals received.

This NOFO will appear on www.grants.gov.