



USAID | UKRAINE

FROM THE AMERICAN PEOPLE

REVISED VERSION OF BAA No. BAA-UKR-CYBERSECURITY-2019 DATED MARCH 6, 2019

Issuance Date: February 15, 2019
Opportunity Number: BAA-UKR-CYBERSECURITY-2019
Deadline for Questions (Round 1): March 4, 2019, 10:00 a.m. Kyiv time
Deadline for Questions (Round 2): March 13, 2019, 10:00 a.m. Kyiv time
Expressions of Interest Due: April 8, 2019, 10:00 a.m. Kyiv time

The USAID Broad Agency Announcement for Cybersecurity for Critical Infrastructure in Ukraine

I. Overview

The United States Agency for International Development (USAID) is issuing this Broad Agency Announcement (BAA) to seek participants to co-create, co-design, co-invest, and collaborate on research and development interventions to address cybersecurity for critical infrastructure in Ukraine. USAID invites the following categories of interested parties to submit Expressions of Interest (EOI) in response to this BAA: (1) Implementing Partners, (2) Co-Investors, and (3) Experts. The description of each category of interested party is provided in Section III, Stage 1 of this BAA.

The intent of the BAA is to foster co-creation and co-design to the maximum extent to create innovative, high quality, effective partnerships in order to implement an activity to address this critical development challenge. USAID will invite selected for-profit and non-profit, public and private organizations, as detailed below, to co-create research and development (R&D) solutions to the Problem and Challenge Statements stated in this BAA, including those organizations that have ideas, expertise, resources, and/or funding to add to potential solutions.

Co-Investing: USAID seeks to align goals with the partners under this BAA, to facilitate shared responsibility, shared risk, and shared resourcing. Shared resourcing requires financing or other resources, both tangible and intangible, such as in-kind contributions, expertise, intellectual property, brand value, high-value coordination, and access to key people, places, and information, are directed towards reaching the solution to the Problem/Challenge. Co-investing does not require the equal investment of resources, such as 1:1 leverage, but rather resource contributions that are appropriate to the specific project's objectives, considering the comparative advantages brought by the participation of each party.

A. Federal Agency Name:

The United States Agency for International Development (USAID) administered by the USAID Mission in Ukraine

B. Opportunity Title:

Cybersecurity for Critical Infrastructure in Ukraine

C. Opportunity Number:

BAA-UKR-CYBERSECURITY-2019

D. Authority:

This BAA is issued under Federal Acquisition Regulation (FAR) Part 35.016 (c). This is not a FAR Part 15 Procurement.

E. Catalog of Federal Domestic Assistance (CFDA) Number:

98.001 USAID Foreign Assistance Programs for Overseas

II. Problem and Challenge Statements

PROBLEM:

Today, conflict between countries is just as likely to play out in cyberspace as it is in physical space. Cybersecurity has emerged as a critical national security challenge for many governments around the world.

Ukraine is on the digital frontlines of a cyberspace war that its President has declared as a critical battlefield for state independence. Alongside a physical war, in which Russia occupies Crimea and supports an ongoing armed conflict in eastern Ukraine, the Kremlin is prosecuting a broader campaign of ‘hybrid warfare’ in Ukraine, in which cyberattacks play a key role. Since 2014, pro-Russia or Russia-supported groups have mounted a number of serious cyberattacks on Ukraine, including on Ukraine’s first post-Euromaidan presidential elections, its power grid, and financial system. These sophisticated attacks were targeted and timed to destabilize the country and decrease domestic -- and international -- confidence in Ukraine’s ability to deliver basic services and security. In these attacks, some of which were the result of multiyear campaigns, the Kremlin enlists the latest information technologies to direct coordinated efforts aimed at inciting social division, disseminating propaganda, and violating the sovereignty and territorial integrity of Ukraine in cyberspace.

In response to large-scale attacks on its critical infrastructure, including its energy, transportation, communication, financial and banking systems, in 2018 the Government of Ukraine (GOU) adopted the Law On the Basic Principles of Cybersecurity of Ukraine and approved the National Cybersecurity Strategy Action Plan. The GOU has taken a number of steps in recent years in order to promote Ukraine’s cyber resilience, including the establishment of the National Cybersecurity Coordination Center in 2016, the engagement in the first

Bilateral Cybersecurity Dialogue between the United States and Ukraine in 2017, and the proposed update of the cybercrime legislation to meet the Budapest Convention requirements, which harmonize national laws to promote multilateral cooperation in combatting cybercrimes. These activities are complemented by strong cooperation with international partners across the cybersphere, including on cybercrime and cyber defense.

CHALLENGES:

Successful attacks on critical infrastructure usually start with unsafe online behavior and practices. Lack of cybersecurity skills among Ukraine's workforce, and insufficient systematic training or resources dedicated to improving cybersecurity within Ukraine's workforce and general population, provides an opening for the Kremlin's aggression and puts the nation's critical infrastructure at risk. These issues are compounded by pervasive outdated hardware and unlicensed software, making Ukraine a major destination for domestic and international cybercrime.

In the context of the ongoing military conflict and the upcoming presidential and parliamentary election season, the GOU has also imposed certain restrictions on internet freedoms in the interests of cybersecurity. These restrictions are strongly criticized by human rights activists and civil society organizations who pointed out the potential for repressive censorship and violations of citizens' rights under the guise of protecting infrastructure and government data. The challenge therefore is to improve cybersecurity of Ukraine's critical infrastructure without violating the rights and freedoms of citizens or facilitating politically based persecutions.

The U.S. Government's (USG) support for advancing cybersecurity in Ukraine is also challenged by persistent corruption in the public sector. Allegations persist that Ukraine's own cybersecurity institutions participated in cyberattacks, and supported the amendment of the Law on Prevention of Corruption to block public access to key public records. These are warning signs that engagement with Ukrainian cybersecurity institutions requires careful risk analysis in the context of the USG's ongoing work to support improved and expanded eGovernance tools to reduce corruption through increased transparency and accountability in Ukraine's public sector.

USAID/Ukraine is seeking to develop and test new and innovative approaches that will concretely address these and other cybersecurity challenges in Ukraine.

III. The BAA Process

The amount of resources made available under this BAA will depend on the concepts received and the availability of funds from USAID and other co-investors. Some award types may not include any funding. Under this BAA, activities will be co-created, co-developed, and finally awarded to interested parties in four stages, including (1) submission of an initial Expression of

Interest (EOI) by interested parties, (2) development of an activity concept paper through initial co-creation and then co-development with USAID, (3) a USAID-led review and selection of activity Concept Papers, and (4) the final award of contract(s) or other agreement(s) to partners. Unless provided otherwise, interested parties are responsible for all costs incurred to prepare its EOI and to participate in co-creation and/or co-development.

Any awards issued under this solicitation will be for Applied Research or Development, as those terms are defined in 48 USC 35.001, as follows:

“Applied research” means the effort that:

- (a) normally follows basic research¹, but may not be severable from the related basic research;
- (b) attempts to determine and exploit the potential of scientific discoveries or improvements in technology, materials, processes, methods, devices, or techniques; and
- (c) attempts to advance the state of the art. When being used by contractors in cost principle applications, this term does not include efforts whose principal aim is the design, development, or testing of specific items or services to be considered for sale; these efforts are within the definition of “development,” given below.

“Development” means the systematic use of scientific and technical knowledge in the design, development, testing, or evaluation of a potential new product or service (or of an improvement in an existing product or service) to meet specific performance requirements or objectives. It includes the functions of design engineering, prototyping, and engineering testing; it excludes subcontracted technical effort that is for the sole purpose of developing an additional source for an existing product.

The steps are detailed as follows:

STAGE 1 - SUBMISSION OF EXPRESSIONS OF INTEREST (EOIs)

USAID invites *Interested Parties* to submit an Expression of Interest (EOI), as provided below. *Interested Parties* are categorized as follows: (1) Implementing Partners, (2) Co-Investors, and (3) Experts. The description of each Interested Party is as follows:

1. Implementing Partner: An implementing partner is an organization that has the capacity and experience to co-design and implement an international development project funded

¹ The primary aim of basic research is a fuller knowledge or understanding of the subject under study, rather than any practical application of that knowledge. (FAR 2.101)

by USAID in connection with the problem statement. USAID expects the implementing partner(s) to lead eventual implementation of the cyber development project.

2. **Co-Investor:** A co-investor is an entity that will contribute financial and/or other resources to the co-creation process and the development project that will address the problem statement. For example, a co-investor could be drawn from a government agency, a foundation, an international organization, a non-government organization, a private business, a think tank, or academic institution, among others.
3. **Experts:** **An expert is a person, team or entity that** has specialized knowledge and experience related to solving the problem statement. Experts could be from academia, government agencies, think tanks, foundations, newspapers, military, private sector companies, international organizations, non-government organizations, among others. Experts must be available for the design process and may participate in the implementation process.

Please submit an Expression of Interest (EOI) addressing the criteria below, in the format required in Section VII. Each interested party is limited to one EOI submission per category. Note: “Category” means (1) Implementing Partners, (2) Co-Investors, or (3) Experts.

USAID will review the EOIs and will select those interested parties that USAID determines to have addressed the evaluation criteria/eligibility stated below, to an extent that demonstrates that the interested party will make a significant contribution to the co-creation.

Interested parties are welcome to form teams with partners, but USAID reserves the right to accept an EOI in its entirety or to select only portions of the EOI, including members of the team. Therefore, USAID recommends that all interested parties submit individual/separate EOIs to ensure they are each being considered. Only one person per EOI may be nominated to represent the interested party, even if that interested party consists of a partnership team that submits one EOI representing all partners of the team.

Not all interested parties that submit an EOI will be invited to proceed to Stage 2. Due to the number of EOIs received, USAID is unable to provide details on why EOIs were not selected.

Criteria for Expressions of Interest:

EOIs received from all interested parties must meet the following criteria:

1. EOIs must indicate the research or development idea which will work towards discovering potential solutions to the Problem and Challenge Statements, by increasing knowledge and understanding of potential solutions, exploiting scientific discoveries or improvements in technology, materials, processes, methods, devices, or techniques, advancing the state of the art, or using scientific and technical knowledge in the design, development, testing, or evaluation of a potential new product or service (or of an improvement in an existing product or service).

2. EOIs must demonstrate the potential to have a significant impact (e.g. lead to a potential breakthrough in improving cybersecurity), that ultimately could achieve that even greater impact at scale.
3. EOIs must indicate the background and expertise of the interested party, and the managerial and technical staff or team engaged in the endeavor.
4. EOIs must indicate what resources are available to be applied toward the solutions identified during the co-design process. Such resources include cash and other resources, both tangible and intangible, such as in-kind contributions, expertise, intellectual property, brand value, high-value coordination, and access to key people, places, and information.
5. USAID will also consider the reputation of an interested party and its past performance in assessing the ability of the organization to contribute to the co-creation of development solutions addressing the issues laid out in the Problem and Challenge Statements.

STAGE 2 - CO-CREATION AND CO-DEVELOPMENT OF THE CONCEPT PAPER

During Stage 2, selected interested parties, based on the EOI submissions, will co-create potential solutions to the Problem and Challenge Statements by brainstorming and innovating solutions and identifying resources, potentially leading to concept papers that USAID or other co-investors will consider for funding.

Co-Creation

USAID will review the EOIs and will select those interested parties that USAID determines have addressed the criteria/eligibility stated within the BAA to an extent that the interested party will make a significant contribution to the Co-Creation process. The Co-Creation process will include USAID, implementing partner(s), co-investor(s), and expert(s).

The Co-Creation process may take the form of a workshop, conference, meeting, or other the method at the discretion of USAID. At this time USAID anticipates having one co-creation workshop in Kyiv, Ukraine from June 3-7, 2019 with the potential for additional workshops. However, USAID reserves the right to make any changes, including, but not limited to, changing the dates of the workshop, changing the location of the workshop, or having additional workshops. Specific details on the method, location, date and time of co-creation for this BAA will be communicated directly to those interested parties invited to participate at a later date. An invitation to co-create is not a guarantee of funding nor is it a guarantee of moving forward to Stage 3.

For more information on co-creation and its design approaches, please see the following link:
<https://usaidlearninglab.org/library/co-creation-discussion-note-ads-201>.

Unless provided otherwise, interested parties are responsible for all costs incurred by the interested party to participate in the Co-Creation process.

Co-Development of Concept Papers

Working together, USAID and the interested parties will collaborate to develop Concept Paper(s), taking a holistic approach to addressing the Problem/Challenge based on insights derived from the Co-Creation process, identifying creative approaches to resourcing projects. Concept Papers will consider and include additional implementing and co-investment partners to complement the project, including reasonable cost sharing, leverage, or other exchange of resource arrangements.

Not all interested parties that participate in the Co-Creation process may be invited to submit a Concept Paper for review by the Peer and Scientific Review Board (Stage 3).

The Concept Paper will further detail and explain the proposed project. Submission requirements for the Concept Papers will be defined at a later date and communicated directly to those interested parties that have been invited to participate in Stage 2.

During this phase, the approaches developed during the Co-Creation process will be refined and submitted to the Peer and Scientific Review Board for review and comments. There are no predetermined number of times the Board will review each concept, neither is the Board obligated to recommend an award for each concept submission.

STAGE 3 - REVIEW BY THE PEER AND SCIENTIFIC REVIEW BOARD

USAID and the interested parties connected with each Concept Paper will present the Concept Paper to the Peer and Scientific Review Board, comprised of experts from USAID, partners, and/or outside parties. The Peer and Scientific Review Board will review Concept Papers and recommend which interested parties should be considered Apparently Successful Partners. Using its technical expertise, the Peer and Scientific Review Board will recommend whether to move forward with the project, including revisions/additions to the project, and interested parties and resources.

Not all interested parties that present a Concept Paper to the Peer and Scientific Review Board will be invited to move to Stage 4.

Evaluation Criteria:

Concept Papers will be evaluated based on, at least, the following criteria:

1. **Idea/Approach:** Novelty, creativity and soundness of the idea/approach and its relevance to the Problem and Challenge Statements.

2. **Partnership Contributions and Value:** Strengths of the organization or consortium as a partner, including ability to make a unique contribution to the challenge issued, and opportunities to leverage additional resources.
3. **Impact:** The likelihood of generating substantial, scalable and sustainable impact on the issues discussed in the Problem and Challenge Statements that can be implemented through a USAID-funded award.
4. **Institutional Capacity:** USAID also will consider the organization's past experience in assessing the ability of the organization to contribute to the co-creation of innovative solutions.

STAGE 4: AWARD DETERMINATION

USAID will review the Peer and Scientific Review Board's recommendations and consider other information, such as resource availability and Agency priorities, and will make a determination whether to move forward with the Concept Paper. For Concept Papers that demonstrate a valid and innovative approach in addressing the Problem/Challenge Statement, the Contracting/Agreement Officer will assess the partner's responsibility and identify the anticipated instrument type to facilitate project design.

Request for Additional Information. USAID will work with partners identified by the Peer and Scientific Review Board, and co-design the project and assist the partner to provide additional information with respect to the proposer's technical approach, capacity, management and organization, past performance, and budget, as well as representations and certifications, as needed.

Final Review and Negotiation. The USAID Contract/Agreement Officer will engage in final review, negotiation, responsibility, cost reasonableness, etc., and will co-develop/craft an award instrument with the Apparently Successful Partner(s). If the Apparently Successful Partner(s) and USAID cannot arrive at a mutually agreeable arrangement, USAID may cancel the project at no cost to the U.S. Government.

Award. Award(s) under this BAA will be made to the Apparently Successful Partner(s) on the basis of their ability to achieve solutions to the issues laid out in the Problem and Challenge statements. The standard clauses or provisions for awards are generally prescribed by law and regulation and will vary considerably by award type. Information regarding clauses and provisions will be offered to the Apparently Successful Applicant(s) when the award type is identified.

IV. Additional Considerations

A. EOIs are not evaluated against other EOIs, but solely on the basis of whether USAID believes that the submitter will be a valuable contributor to the co-creation process. USAID may limit the number of initial submissions selected to move forward at its sole discretion.

B. Concept Papers are not evaluated against other Concept Papers, but solely based on USAID's determination that the Concept Paper will successfully address the issues laid out in the Problem and Challenge statements. USAID may limit the number of Concept Papers selected to move forward at its sole discretion based on efficiencies or resource availability.

C. Decisions regarding USAID's pursuit of a particular project, technology or relationship are based on all available information, evidence, data, and resulting analysis.

D. Eligibility Information. Public, private, for-profit, and nonprofit organizations, as well as institutions of higher education, public international organizations, non-governmental organizations, U.S. and non-U.S. governmental organizations, multilateral and international donor organizations, and individuals (in the *expert* category of interested parties only) are eligible under this BAA. All organizations must be determined to be responsive to the BAA and sufficiently responsible to perform or participate in the final award type.

E. Funding availability and amounts will depend on the ideas generated during the collaboration process as well as the funding capacity of participating organizations, which are not necessarily limited to USAID.

V. Specific Rights Reserved for the U.S. Government under this BAA

The U.S. Government reserves specific rights, in addition to rights described elsewhere in this document or by law or regulation, including:

1. The right to award multiple awards, a single award, or no awards.
2. The right to make award without discussions, or to conduct discussions and/or negotiations, whichever is determined to be in the Government's interest.
3. The right to accept submissions (including, but not limited to, EOIs, concept papers, proposals, or applications) in their entirety or to select only portions of submissions for award or co-investment. For example, if an interested party proposes a team of partners, USAID reserves the right to select the interested party with or without all or some of its partners.
4. The right to select for award an instrument type that is appropriate to the specific development context, partner relationship, and concept paper selected for award. Instrument types include, but are not limited to, contracts, grants, cooperative agreements, public-private partnerships, Inter-Agency Agreements, Government to Government Agreements, Donor to Donor Agreements, and Memorandums of Understanding. In addition, the Government may craft a new instrument type to meet the needs of a specific relationship.

5. The right to co-create projects with one or more **interested parties** under the BAA, when it is in the best interest of the Government.
6. The right to request any additional, necessary documentation upon initial review. Such additional information may include, but is not limited to, a further detailed **submission**, budget, and representations and certifications.
7. The right to fund or co-invest in proposals in phases, with options for continued work at the end of one or more of the phases.
8. The right to award instruments under this BAA that do not commit or exchange monetary resources.
9. The right to remove organizations from the BAA process if USAID determines it is no longer in the best interests of the Government to proceed with the organization.

VI. Information Protection:

USAID's goal is to facilitate research and development that will lead to innovative, and potentially commercially viable, solutions. Understanding the sensitive nature of submitters' information, USAID will work with organizations to protect intellectual property. Expressions of interest should be free of any intellectual property that submitter wishes to protect, as the expressions of interest will be shared with USAID partners as part of the selection process. However, once submitters have been invited to advance beyond co-creation, submitters can work with USAID to identify proprietary information that requires protection.

Therefore, organizations making submissions under this BAA grant to USAID a royalty-free, nonexclusive, and irrevocable right to use, disclose, reproduce, and prepare derivative works, and to have or permit others to do so to any information contained in the Expressions of Interest submitted under the BAA. If USAID further engages with the organization regarding its submission, the parties can negotiate further intellectual property protection for the organization's intellectual property.

Organizations must ensure that any submissions under this BAA are free of any third party proprietary data rights that would impact the license granted to USAID herein.

VII. Expression of Interest Information Formatting

GENERAL REQUIREMENTS APPLICABLE TO ALL INTERESTED PARTIES

Expression of Interest (EOI) Information must:

- A. Be in English, no more than ten (10) pages in length and no smaller than 12 point font.

Notes:

- o Fonts smaller than 12 point may be used in text boxes, graphics and tables, as appropriate. USAID requests 12 font minimums in order to ensure submissions are easily legible. Please ensure that text boxes, graphics and tables are easily legible by reviewers.
 - o All required aspects of the EOI must be combined into a single, searchable PDF, and the page limitation will be calculated by the total number of pages of the entire PDF. USAID will not review information submitted above this page limit.
 - o The resume counts towards the ten-page limit of the EOI. Only one resume is required, but Interested Parties are welcome to describe additional team members elsewhere in their EOIs, as applicable.
- B. Be submitted electronically to eparinova@usaid.gov and ashatokhina@usaid.gov and clearly indicate in the subject line of the email the BAA number (BAA-UKR-CYBERSECURITY-2019) and whether the submission falls under the Implementing Partner, Co-Investor or Expert category.
- C. **The first page of the EOI must** contain the following information (included in the page count):
- a. Interested Party Category (Implementing Partner, Co-Investor, or Expert)
 - b. Name and Contact Information of Interested Party
 - c. **Include a contact person for the EOI, including his/her name (both typed and signed), title or position with the organization, address, telephone, and email address);**
 - d. Response Title;
 - e. BAA Name/Number (Cybersecurity for Critical Infrastructure in Ukraine/BAA-UKR-CYBERSECURITY-2019).
 - f. All required aspects of the technical proposal as noted below must be combined into a single, searchable PDF, and the page limitation will be calculated by the total number of pages of the entire PDF.
- D. Be in .pdf format.

SPECIFIC REQUIREMENTS APPLICABLE TO A PARTICULAR INTERESTED PARTY

Expression of Interest (EOI) must include the following information:

1. Implementing Partner:

- a. RESEARCH AND DEVELOPMENT (R&D) IDEA: EOIs must indicate the R&D idea which will address the issue laid out in the Problem and Challenge Statements, by increasing knowledge and understanding of potential solutions, exploiting scientific discoveries or improvements in technology, materials, processes, methods, devices, or techniques, advancing the state of the art, or using scientific and technical knowledge in the design, development, testing, or evaluation of a potential new product or service (or of an improvement in an existing product or service). The idea must demonstrate the potential to have a

significant impact (e.g. lead to a potential breakthrough in improving cybersecurity), that ultimately could achieve even greater impact at scale.

- b. **COLLABORATION:** EOIs must describe how the implementing partner will help bring together the co-design team to develop a cohesive concept paper for a development project that will address the problem statement.
- c. **RESOURCES:** EOIs must indicate what resources are available to bring to bear on the co-design and solution. Such resources include both tangible and intangible, such as expertise, intellectual property, brand value, high-value coordination, access to key people, information, cash, and in-kind contributions.
- d. **EXPERIENCE:** EOIs must discuss the implementing partner's experience in implementing cyber security development projects and the implementing partner's experience in Ukraine and/or similar environments. EOIs must include at least three relevant references, including the following information: Name; email address and phone number; and projects under which the interested party collaborated with the named reference.
- e. **RESUME:** EOIs must include a professional resume of the person who will represent the implementing partner on the co-design team. Only one individual may be nominated to represent the interested party at the co-creation workshop. Three references must also be provided for the proposed representative. References must include: Name; email address and phone number; and the capacity under which the representative collaborated with the named reference.

2. Co-Investor:

- a. **RESEARCH AND DEVELOPMENT (R&D) IDEA:** EOIs must indicate the R&D idea which will address the issue laid out in the Problem and Challenge Statements, by increasing knowledge and understanding of potential solutions, exploiting scientific discoveries or improvements in technology, materials, processes, methods, devices, or techniques, advancing the state of the art, or using scientific and technical knowledge in the design, development, testing, or evaluation of a potential new product or service (or of an improvement in an existing product or service). The idea must demonstrate the potential to have a significant impact (e.g. lead to a potential breakthrough in improving cybersecurity), that ultimately could achieve even greater impact at scale.
- b. **CO-INVESTING:** EOIs must describe the co-investing resources that the co-investor will contribute to the development project as well as any conditions, restrictions, and limitations to be placed on the resources. Such resources include cash and other resources, both tangible and intangible, such as in-kind

contributions, expertise, intellectual property, brand value, high-value coordination, and access to key people, places, and information.

- c. **REASON:** EOIs must describe why the co-investor seeks to participate on the co-design team, including any proposed research and development ideas they would be interested in co-financing. The R&D idea which will work towards discovering potential solutions to the Problem and Challenge Statements, by increasing knowledge and understanding of potential solutions, exploiting scientific discoveries or improvements in technology, materials, processes, methods, devices, or techniques, advancing the state of the art, or using scientific and technical knowledge in the design, development, testing, or evaluation of a potential new product or service (or of an improvement in an existing product or service). The idea must demonstrate the potential to have a significant impact (e.g. lead to a potential breakthrough in improving cybersecurity), that ultimately could achieve that even greater impact at scale.
- d. **COLLABORATION:** EOIs must describe how the co-investor will contribute to the co-design team to develop a cohesive concept paper for a development project that will address the problem statement.
- e. **RESUME:** EOIs must include a professional resume of the person who will represent the co-investor on the co-design team. **Only one individual may be nominated to represent the interested party at the co-creation workshop.** Three references must be provided for the proposed representative. References must include: Name; email address and phone number; and the capacity under which the representative collaborated with the named reference.

3. Experts:

- a. **RESEARCH AND DEVELOPMENT (R&D) IDEA:** EOIs must indicate the R&D idea which will work towards discovering potential solutions to the Problem and Challenge Statements, by increasing knowledge and understanding of potential solutions, exploiting scientific discoveries or improvements in technology, materials, processes, methods, devices, or techniques, advancing the state of the art, or using scientific and technical knowledge in the design, development, testing, or evaluation of a potential new product or service (or of an improvement in an existing product or service). The idea must demonstrate the potential to have a significant impact (e.g. lead to a potential breakthrough in improving cybersecurity), that ultimately could achieve that even greater impact at scale.
- b. **EXPERTISE:** EOIs must describe what expertise they will bring to the co-design team and why the expert wishes to participate.

- c. RESUME: EOIs must include a professional resume of the expert, including publications, consultancies, special projects, and three references. **Only one individual may be nominated to represent the interested party at the co-creation workshop.** References must include: Name; email address and phone number; and the capacity under which the expert collaborated with the named reference.
- d. COLLABORATION: EOIs must describe how the expert will contribute to the co-design team to develop a cohesive concept paper for a development project that will address the problem statement.
- e. RESOURCES: EOIs must describe the material support, if any, that the expert's institution will make available to the expert to facilitate the co-design process at all stages of project design. Such resources include both tangible and intangible, such as expertise, intellectual property, brand value, high-value coordination, access to key people, information, cash, and in-kind contributions.
**If the institution is unable to fund the expert to attend the co-design workshop, USAID might be able to provide this support. If the expert's institution is unable to fund the travel, the EOI must explain why USAID should consider funding the travel.*

VIII. Obtaining the BAA

This BAA can be downloaded from <http://www.grants.gov> and <http://www.fbo.gov>. Issuance of this BAA does not constitute an award commitment on the part of USAID, nor does it commit USAID or any of its funding Partners to pay for costs incurred in the preparation and submission of EOIs and Concept Papers. Further, USAID reserves the right to reject any or all EOIs and Concept Papers received.

IX. Questions

Questions regarding this BAA must be submitted electronically to eparinova@usaid.gov and ashatokhina@usaid.gov by the date and time specified on page 1. Answers to questions will be provided in an amendment to the BAA. The subject line of the email should indicate the BAA number: BAA-UKR-CYBERSECURITY-2019.

X. References

The following is a list of attachments to this BAA solicitation that provide useful reference materials and background information related to the subject matter.

[1] National Cyber Strategy of the United States of America. September 20, 2018, p. 24.
Accessed online: <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>

[2] Decree of the President of Ukraine No. 126/2018 “Concerning the Decision of the Council of National Security and Defense of Ukraine dated May 2, 2018 "On the Application and Revocation of Personal Special Economic and Other Restrictive Measures (Sanctions)".

Accessed online: <http://www.rnbo.gov.ua/documents/473.html>

[3] 115th Congress 2D Session S. 2455 “A Bill To encourage United States-Ukraine cybersecurity cooperation and require a report regarding such cooperation, and for other purposes.” February 27, 2018. Accessed online:

<https://www.congress.gov/115/bills/s2455/BILLS-115s2455is.pdf>

[4] “On Approval of the Action Plan for 2018 on the Implementation of the Cybersecurity Strategy of Ukraine.” Accessed online: <http://zakon0.rada.gov.ua/laws/show/481-2018-%D1%80>

[5] 2017 Doctrine of Information Security of Ukraine. Ratified by the President of Ukraine on 25 February 2017. Accessed online: <http://zakon3.rada.gov.ua/laws/show/47/2017>

[6] “Cybersecurity Strategy of Ukraine”. Accessed online:

<http://zakon0.rada.gov.ua/laws/show/96/2016/paran11#n11>

[7] The Convention on Cybercrime of the Council of Europe (CETS No.185), also known as the ‘Budapest Convention’. Accessed online: <https://www.coe.int/en/web/cybercrime/the-budapest-convention>

[8] Worldwide Threat Assessment of the US Intelligence Community, Statement for the Record by Daniel Coats, Director of National Intelligence, January 29, 2019. Accessed online:

<https://www.intelligence.senate.gov/sites/default/files/documents/os-dcoats-012919.pdf>

[9] U.S. Department of Homeland Security guidance on Critical Infrastructure Sectors.

Accessed online: <https://www.dhs.gov/cisa/critical-infrastructure-sectors>