Cyber Security Improvement Grant (CySIG)

ENGLISH

Purpose:	**To upgrade the level of information and cyber security at Academic & Research Institutions.** Grants are intended to enhance the capacity of academic and research institutions to defend against and respond to cyber threats posed by malicious entities seeking to steal sensitive research and design-data through unauthorized access to computer systems.
Competition Opens:	**Georgia: June 9, 2022** **Armenia: September 29, 2022** **Turkey, Azerbaijan, Bulgaria: September 23, 2022**
Application Deadline:	**Georgia: July 22, 2022** **Armenia, Turkey, Azerbaijan, Bulgaria: November 7, 2022**
Eligibility:	Applicants – Academic & Research Institutions - with areas of advanced research on topics such as: • Science and technology • Engineering (all types) • Social sciences • Medical • Computing • Navigation and Avionics • Propulsion Systems • Telecommunications and Information Security • Electronics Eligible countries – Georgia, Armenia, Turkey, Azerbaijan, Bulgaria
How to Apply:	By email to cysig@crdfglobal.org
General Area:	Cyber Security
Award Amounts:	Up to $30,000
Award Duration:	One year
Announcement & Application:	http://www.crdfglobal.org/ (see "Current Funding Opportunities")

Overview

Obtaining the knowledge, skills, and tools for a successful cybersecurity program through a workshop needs to be augmented with capacity-building to implement recommended controls and safeguards. CRDF Global will award grants to research institutions and universities that have sent representatives to one of the workshops for equipment—and associated installation fees—, materials, and supplies that improve information and cyber security.

- Cyber Security Improvement Grants are CRDF Global-sponsored grants to upgrade the level of information and cyber securityat Academic & Research Institutions that match eligibility criteria
- CySIGs are a one-time, one-year award of up to $30,000 each
- The awards are implemented through CRDF Global

Eligibility

Any research institution or institution of higher learning that has sent a representative to one of the program workshops on cyber theft are eligible to apply. Applicants may apply as an individual institution or as a consortium. The Principal Investigator and other members of the research grant team do not need to have attended the workshop. For applications to be considered for this competition, institutional approval is required.

CySIGs are open to applicants—public and private academic and research institutions enterprises—that possess all from the listed criteria:

- Active research on topics listed above. Candidates from other research topics may apply with proper justification.
- An existing IT infrastructure appropriate for advanced security enhancements
- Physical in-person presence within any of the eligible countries
- Institutional approval

Each proposal is evaluated independently and therefore should not be part of, nor depend on the success of, other proposals submitted to this program.

Each applicant—institution—is allowed to submit only one application per research department to this grant competition.

CRDF Global reserves the right to restrict the participation of any individual or institution in its programs. CRDF Global complies with all U.S.A laws and regulations pertaining to export control and the participation of foreign nationals or institutions in its activities. It is the policy of CRDF Global not to conduct any transactions with U.S. restricted entities without appropriate authorization from the U.S. Government.

Required Application Materials

All applications should include the information and supporting documents in CRDF Global's *Countering Cyber Theft in Academia Grant Application Checklist* which can be downloaded as a Microsoft Word document template. Application materials and research products can either be submitted in English or in a standardized national language. The items in the application and narrative should be limited to five single-spaced pages. Additional supporting documents and spreadsheets can be appended to this narrative or sent as separate documents.

A completed CySIG application form and supporting documents including:

- **A completed CySIG budget form*** (*mandatory*)
- **The Curriculum Vitae (CV)** of each project team member from the applicant' side—3 pages eachmaximum, in Word or PDF format - with indicated contact phone and e-mail of Chief Information Security Officer (CISO) from the applying institution (*mandatory*)
- **An internal or external cybersecurity vulnerability assessment—**in form of a report or internal memo (*mandatory*)
- **Institutional Letter of Endorsement** *(mandatory)*to qualify, a document from your institution's leadership must state that you have support from your institution to apply for and implement this grant. Form* ***must*** *be signed by leadership.*
- **A list references** must be provided of independent individuals who are familiar with the work of the Principal Investigator or project team

All application materials must be submitted as attachments in Word or PDF files using the forms provided by CRDF Global.

Coverage of the Grant

*CySIGs are intended for **equipment (and associated installation fees), materials, and supplies** that improve information and cyber security. **The labor costs of the project team members from applicant's side are not allowed under this grant funding.**

Allowable Costs

The maximum total grant is up to $30,000 U.S. Dollars (USD) from CRDF Global awarded directly to the institute at which the Primary Point of Contact is employed at. *In case of an award, budgets requesting CRDF Global funding may be subject to revisions.

Allowable Expenses

- Equipment, Supplies, and Services (ESS),
- Other Direct Costs (other collateral expenses that may occur in relation with ESS installation andmaintenance)

Proposal Evaluation Criteria

All proposals will be evaluated based on the following criteria:

1. Cyber security relevance and impact:

- What are the proposed security upgrades and how will they improve security within the institution?
- How often did the applicant observe precedents of cyber-attack attempts aimed on its informational resources?
- What are the maximum possible consequences in case of a successful cyber-attack / cyber theft on key information resources?

2. Sustainability and commitment:

- Does the applicant's organization demonstrate their commitment to the project by offering anycomplimentary financial, logistical, and/or personnel support?
- Does the applicant have a clear monitoring/evaluation strategy or plan? How will the applicant know that the requested upgrade has had the intended impact?
- Does the applicant institution offer long-term financial support or a detailed maintenance plan?

3. Clarity, feasibility, and detail:

- Does the project have a clear and reasonable timeline and plan for implementation?
- Is the proposed budget appropriate and reasonable for the activities?
- Is the institution's current information and telecommunications system appropriate for the proposed upgrades?

4. Past Performance:

- Does the applicant have a record of high-quality research on matters relating to responsible scientific and research ethics, integrity, information security, data governance, responsible technology, institutional compliance, knowledge of dual-use technology and export controls?

5. Budget:

- Has the applicant mapped the activities and tasks in the proposal to the project budget?
- Is the project budget sufficient to conduct the tasks in the proposal during the proposed period of performance?
- Do the budget line items represent reasonable and customary costs and a proper balance between direct and indirect costs?

Please note that CySIGs are competitive grants and repeated funding for the same individuals or institutions is limited.

Additional Information

- For detailed information regarding the CySIG competition please visit: https://www.crdfglobal.org/docs/default-document-library/cysig-faq.docx
- For detailed information regarding general CRDF Global grant policies please visit:http://www.crdfglobal.org/grants-and-grantees/faqs+
- For additional questions regarding the CySIG competition please contact CRDF Global at cysig@crdfglobal.org

How to apply

- Submit completed application, budget and requested documents to **cysig@crdfglobal.org**.

CRDF GLOBAL POLICIES

Anti-Plagiarism: CRDF Global will not provide funding to an application in which plagiarism exists. All applications for funding submitted to CRDF Global will be thoroughly screened for plagiarism against a large number of sources including published research papers, books, conference abstracts, and websites. When plagiarism is detected, the program within CRDF Global that is overseeing the funding opportunity will determine the specific action to be taken. Action taken may include but is not limited to a) informing the applicant that plagiarism has been discovered; b) excluding the applicant from the funding opportunity; c) informing the applicant's institution; d) informing reviewers; e) informing organizations collaborating with CRDF Global on the funding opportunity; f) barring the applicant from

participation in future fundingopportunities.

CySIG Project Examples

***Please note that CySIGs will not fund training or workshop events. CySIGs will only fund trainings associated with using the procured cyber security equipment or understanding cyber security procedures.**

Examples of equipment to be used for ensuring cyber security of information & telecommunicationsystems (ITS) and for physical security of objects of information activity (OIA) include:

1. Systems of access control to objects of information activity (OIA) and/ or server rooms (e.g., cameras,electronic digital locks)
2. Web Application Protection Screen (WAF)
3. Firewall (network firewall)
4. Intrusion Prevention Systems (IPS)
5. Security Information and Security Event Management (SIEM) systems (for example, McAfeeEnterprise Security Manager)
6. Antivirus software

***Please note that the above is not an exhaustive list of eligible projects. CRDF Global encourages applicants to contact cysig@crdfglobal.org if they have any questions or concerns regarding the eligibilityof a potential topic.**

Examples of activities and procedures for establishing or enhancing cybersecurity:

1. Audit and development of IT management processes (for example, based on COBIT 5 methodology)
2. Information security audit and recommendations development of based on it (for example, based on ISO 270XX package of standards)
3. Development and implementation of information security incident management procedures (policies)
4. Development and implementation of a procedures (policies) for changes management in information systems
5. Development and implementation of procedures (policies) of information resources control access
6. Training and certification of information security department staff in accordance with international requirements (for example, certification by one of the ISACA program