Cyber Security Improvement Grant (CySIG)
Program Announcement

Purpose:	To enhance cyber security at organizations in order to secure dual-use or weapons proliferation-sensitive information
Competition Opens:	May 1, 2022
Application Deadline:	September 30, 2022
Eligibility:	Applicants – academic, research (private and public), government-owned enterprises and government agencies, private companies from the following countries: Georgia, Indonesia, Malaysia, Morocco, Philippines, Vietnam, Cambodia, Thailand, Poland, Romania
How to Apply:	By email to dkuznetsova@crdfglobal.org
General Area:	Cyber Security
Award Amounts:	Up to $50,000
Award Duration:	Until December 30, 2022
Announcement & Application:	http://www.crdfglobal.org (see "Current Funding Opportunities")

Overview

- CySIGs are CRDF Global-sponsored grants to secure proliferation-sensitive information and technology to prevent cybertheft from private, research and academic sectors in Southeast Asia, Europe, and Morocco.
- CySIGs are a one-time award of up to $50,000 each.
- The awards are implemented through CRDF Global.

Eligibility

CySIGs are open to applicants - academic, research (private and public), government-owned enterprises and government agencies, private companies from Georgia, Indonesia, Malaysia, Morocco, Philippines, Vietnam, Cambodia, Thailand, Poland, Romania - that possess all from the listed criteria:

- A citizen and consumer-oriented web-interface
- An existing IT infrastructure appropriate for advanced security enhancements
- Generate, hold and/or access dual-use, WMD-enabling and/or weaponizable information, data or technology related to artificial intelligence (AI) and associated fields (e.g. machine learning, neural networks), biotechnology, semiconductor manufacturing, and high-performance computing

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 is allowed to submit **only one application** per this grant competition. One institution can submit multiple applications if from a different department.

<u>CRDF Global reserves the right to restrict the participation of any individual or institution in its programs.</u>
CRDF Global complies with all U.S. 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 the appropriate authorization from the U.S. Government.

Required Application Materials

- **A completed CySIG application form** (*mandatory*)
- **A completed CySIG budget form*** (*mandatory*)
- **The curriculum vitae (CV)** of the Chief Information Security Officer (CISO) of the applying institution (or relevant specialist) – 3 pages maximum, in Word or PDF format - with indicated contact phone and e-mail (*mandatory*)

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

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

Allowable Costs

The maximum total grant amount is up to **$50,000** (USD) awarded directly to the institution or in the in-kind form if the procurement is proceeded directly by CRDF Global. *In case of an award, budgets requesting CRDF Global funding may be subject to revision.

Allowable Expenses include:

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

Proposal Evaluation Criteria

All proposals will be evaluated based on the following criteria:

Dual-use relevance:

- Does the applicant's organization generate, hold, and/or access dual-use, WMD-enabling, and/or weaponizable information, data, or technology?

Cyber security relevance and impact:

- What are the proposed security upgrades and how will they improve security within the applicant organization?
- 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 on key information resources?

Sustainability and commitment:

- Does the applicant's organization demonstrate its commitment to the project by offering any complimentary 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?

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?

- Will interruptions in work with the web interface or information resource (network) directly impact services provided by the government institution/s and state-owned enterprise/s?
- Is the institution's current information and telecommunications system appropriate for the proposed upgrades?

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/funding-opportunities/
- For detailed information regarding general CRDF Global grant policies please visit: https://www.crdfglobal.org/grants/information-applicants
- For additional questions regarding the CySIG competition please contact CRDF Global at dkuznetsova@crdfglobal.org

How to apply

- Submit completed application, budget and requested documents to dkuznetsova@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 funding opportunities.

Confidentiality of Proposals and Applicant Information: CRDF Global assures confidentiality of all proposals' material and will require all panelists and reviewers to respect the confidentiality of proposals. However, proposal authors should be aware that successful proposals will be treated as public information. Therefore, at the author's discretion, if there is specific information in the proposal that is business-confidential and not intended for public dissemination, it should be clearly labeled as such. Such passages will be withheld from public distribution if the proposal is successful.

CySIG Project Examples

*** Please note that CySIGs will not fund training or workshop events.**

Examples of equipment to be used for ensuring cyber security of information & telecommunication systems (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, McAfee Enterprise Security Manager)

6. Advanced malware protection
7. Equipment for physical security assurance and work continuity of server rooms and data centers (backup power supply, fire alarm, fire extinguishing system, climate system)
8. Endpoint Detection and Response.
9. Access Control (e.g., developing an acceptable use policy, least-privileged user accounts, configuring user accounts and security permissions within multiple environments)
10. Media Protection (e.g., properly sanitizing or destroying media)
11. Physical Protection (e.g., establishing physical access control)
12. System and Communications Protection (e.g., monitoring external and internal boundary devices, implementation of subnets)
13. System and Information Integrity (e.g., identification of system issues, deployment of network/host-based signatures, performance of periodic anti-virus scanning)

***Please note that the above is not an exhaustive list of eligible projects. CRDF Global encourages applicants to contact dkuznetsova@crdfglobal.org if they have any questions or concerns regarding the eligibility of 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 based on it (for example, on the basis of ISO 270XX package of standards)
3. Development and implementation of information security incident management procedures (policies)
4. Development and implementation of 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 programs)