CRITICAL INFRASTRUCTURE DIGITALIZATION AND RESILIENCE

PROGRAM DESCRIPTION

Countries in Europe and Eurasia are facing more diverse and complex cyberattacks targeting critical infrastructure. In response, the Critical Infrastructure Digitalization and Resilience (CIDR) program is assisting partner governments to protect infrastructure such as energy, telecom, finance, and e-services as well as key institutions from these malicious attacks. Ultimately, CIDR aims to help the region improve its cybersecurity posture so critical infrastructure entities are more resilient and can continue to provide citizens with essential services.

Specifically, CIDR's country teams collaborate with local partners to build national cybersecurity resilience, working with stakeholders from government, critical infrastructure, academia, civil society, and the private sector. CIDR's activities include targeted technical assistance, support for cybersecurity laws and regulatory agencies, and capacity building to grow and strengthen cybersecurity workforces in the region. These activities along with robust information sharing are helping to create more secure societies where people can safely work, connect, and thrive.

Meeting of the Moldova Critical Infrastructure Cybersecurity Working Group, September 2023

CIDR GOALS

CIDR works with diverse stakeholders from throughout a country's cybersecurity ecosystem. CIDR aims to:

- **Accelerate** cybersecurity workforce development
- **Empower** organizations to identify and address cybersecurity threats
- **Strengthen** cybersecurity governance
- **Facilitate** the sharing of cyber threat information

CIDR COUNTRIES

Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Georgia, Kosovo, Moldova, Montenegro, North Macedonia, Serbia, and Ukraine.

LIFE OF ACTIVITY

10/2021 – 09/2026

USAID FUNDING

$29,997,925

IMPLEMENTING PARTNER

DAI Global, LLC

PRIMARY ACTIVITIES

Accelerating workforce development: Countries in Eastern Europe face a growing demand for cybersecurity professionals; CIDR is helping build the supply of qualified cybersecurity job candidates.

- CIDR's market-driven data is being used in Georgia and North Macedonia to train professors and instructors and to update university and vocational cybersecurity education.
- CIDR's Cyber Pathways for Women activities in Moldova, North Macedonia, and Serbia work with government, business, academia, training institutions, and civil society to break down barriers and create pathways to cyber careers and a more gender-inclusive cybersecurity environment.

Empowering entities to identify and address threats: CIDR provides targeted assistance to the critical infrastructure and key institutions on which countries depend.

- In Albania and Moldova, CIDR facilitated hardware and software upgrades and tailored training that increased the capacity of government partners to detect and defend themselves from cyberattacks.
- In Georgia, Kosovo, and North Macedonia, CIDR works with institutions to implement U.S.- and EU-standard information security management systems to identify and mitigate risks and protect data.

Facilitating cybersecurity governance: CIDR builds communication and consensus by facilitating Critical Infrastructure Cybersecurity Working Groups in Albania, Kosovo, Moldova, and North Macedonia.

- These working groups are chaired by top government appointees who convene key officials from government, critical infrastructure, academia, civil society, and the private sector.
- Group members use "roadmaps" meeting-to-meeting to build common understanding, deliberate cybersecurity legislation, policy, and oversight, and submit recommendations to government.
- CIDR is advising on the creation of national cybersecurity authorities in Kosovo, Moldova, and North Macedonia and on the drafting of national cybersecurity strategies and institution-specific bylaws.
- In Georgia, CIDR supports a sectoral cybersecurity working group focused on the financial sector.

Establishing information-sharing networks: CIDR builds capacity within national cybersecurity coordination bodies to manage and coordinate responses to cybersecurity incidents, threats, attacks, and mitigation.

- In North Macedonia, CIDR partnered with the Agency for Electronic Communications to conduct the National Coordination Exercise, tabletop exercise, and hands-on technical drill, providing training for the country's Cybersecurity Incident Response Team (CSIRT) and critical infrastructure operators.
- In Kosovo and Moldova, CIDR is supporting the establishment of the countries' national cybersecurity authorities, which will oversee cyber emergency response and mitigation and cybersecurity information management, among other responsibilities.

Public Hearing in Skopje, North Macedonia, for the 2023-2027 National Cybersecurity Strategy and Action Plan.

CONTACTS: Mina Hasaj, Agreement Officer's Representative, mhasaj@usaid.gov
Erica Bustinza, CIDR Program Director, ebustinza@dai.com