USAID
FROM THE AMERICAN PEOPLE

DAI
Shaping a more livable world.

CRITICAL INFRASTRUCTURE DIGITALIZATION AND RESILIENCE

BACKGROUND

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 from these malicious attacks. CIDR implements select activities for USAID, including initiatives with USAID/Moldova to address cyber governance, workforce development, and other needs.

MOLDOVA FOCUS

CIDR/Moldova works with government ministries and institutions and other key partners. CIDR provides assistance to the Moldovan government and its partners to: 1) lead multi-stakeholder working groups that build consensus around cybersecurity priorities within critical infrastructure, 2) promote sharing of cybersecurity data, 3) bolster the cyber workforce, and 4) build cybersecurity capacity for critical infrastructure operators.

Prime Minister of Moldova, left at the table, shakes hands with the U.S. Ambassador during a presentation at the CIDR-facilitated Critical Infrastructure Cybersecurity Working Group.

CIDR GOALS

CIDR works with national governments, critical infrastructure operators, the private sector, academia, oversight bodies, and regional experts. 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 PROGRAM

10/2021 – 09/2026

USAID FUNDING

$29,997,925

IMPLEMENTING PARTNER

DAI Global, LLC

PRIMARY ACTIVITIES

Facilitate stakeholder collaboration. The multi-stakeholder, government-led and CIDR-facilitated Critical Infrastructure Cybersecurity Working Group discusses key issues and develops understanding and recommendations for strengthening national cybersecurity.

Assist critical infrastructure entities. CIDR helps key infrastructure to understand their cybersecurity postures, supports them in the process of mitigating weaknesses, and seize on opportunities to build resilience against disruptions to information systems.

Build cybersecurity capacity. CIDR assesses the capacity of technologists and cybersecurity specialists at critical infrastructure entities and provides them with training and playbooks to increase readiness for future cyberattacks.

Promote talent sharing. CIDR is exploring mechanisms to allow private sector critical infrastructure operators' experts to sustainably contribute to the national cybersecurity talent pool development via existing academic institutions.

ANTICIPATED RESULTS

GOVERNMENT, CRITICAL INFRASTRUCTURE ALIGNED: EU-standard cybersecurity is understood and mandated across entities in Moldova; cybersecurity laws, support, and compliance are helping to create an enduring and resilient cybersecurity ecosystem.

VIBRANT CYBER CAREER PATHWAYS: Academia, employers, and government officials are collaborating to create and nurture pathways to and within Moldova's cybersecurity workforce.

PUBLIC-PRIVATE TALENT SHARING: A facility is established that enables private sector cybersecurity talent to be utilized by critical infrastructure entities that are resource constrained.

SELF-SUSTAINING CAPACITY DEVELOPMENT: Critical infrastructure entities are assessed and roadmaps are developed for building their cybersecurity capacities; CIDR is assisting operators to implement and refine the roadmaps into sustainable and resilient working models.

CONTACT: CIDR-Moldova@dai.com