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) regional program is assisting partner governments and institutions to protect infrastructure such as energy, telecom, finance, and e-services from these malicious attacks. USAID, through CIDR, supports Georgia to improve cybersecurity governance, develop cybersecurity workforce, and other needs.

GEORGIA FOCUS

The USAID CIDR program in Georgia works with government institutions, the private sector, and other key stakeholders. This activity provides assistance to: 1) facilitate working groups where stakeholders discuss sectoral cybersecurity needs—particularly for the financial sector—and inform state policy and decision making, 2) develop cybersecurity training and the cyber workforce, 3) facilitate development of sectoral cybersecurity policy, and 4) empower organizations to identify and address cybersecurity threats.

CIDR GOALS

The CIDR program 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. CIDR facilitates multi-stakeholder cybersecurity working groups with representatives from public and private entities who deliberate key issues and define priorities for strengthening cybersecurity resilience in the financial sector.

Develop policy. CIDR supports the financial sector in identifying sectoral cybersecurity gaps in legal, policy, and industry standards and provides technical assistance, knowledge transfer, and guidance for developing sectoral sub-laws, policies, and standards.

Empower organizations to identify and address cybersecurity threats. CIDR assists banking and finance institutions to build their capacities to identify and address cybersecurity threats and vulnerabilities.

Accelerate cybersecurity workforce development. CIDR is contributing to strengthening the capacity of Georgia's higher education and training institutions to deliver market-driven cybersecurity skills; CIDR also promotes interest in cybersecurity as a career option and provides practical experience by conducting cybersecurity competition among multi-disciplinary student teams.

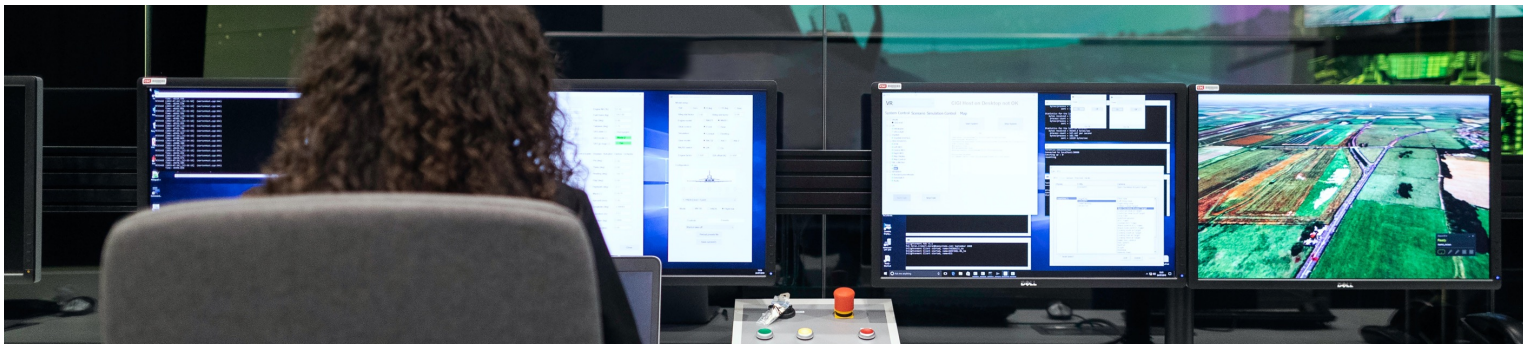
ANTICIPATED RESULTS

STANDARDS ESTABLISHED: Sectoral critical infrastructure regulations and cybersecurity standards are established, improved, and/or implemented, helping to create an enduring and resilient cybersecurity ecosystem.

MARKET-DRIVEN CYBER EDUCATION: Georgia's higher education and training providers are teaching market-driven cybersecurity courses and skills and offering practical learning tools to more students, building the supply of skilled cybersecurity personnel available to critical infrastructure and key institutions.

MORE RESILIENT CRITICAL INFRASTRUCTURE: Sectoral critical infrastructure entities possess strengthened capabilities for identifying and responding to cybersecurity threats.

CYBERSECURITY COLLABORATION ENHANCED: Public and private critical infrastructure stakeholders are actively collaborating and coordinating to build broad-based national cybersecurity.



CONTACT: CIDR-Georgia@dai.com