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 and institutions to defend infrastructure such as energy, telecom, finance, and e-services from these malicious attacks. CIDR implements activities for USAID, including initiatives in North Macedonia to address cyber governance, cyber workforce shortages, and other needs.

## NORTH MACEDONIA FOCUS

CIDR/North Macedonia works with government ministries and institutions and other key partners. The activity provides assistance to: 1) establish legal frameworks as well as coordination bodies where stakeholders deliberate on national cybersecurity needs and inform government policy and decision making, 2) develop the cyber workforce in collaboration with the UK Foreign, Commonwealth & Development Office, 3) facilitate cybersecurity information-sharing networks among the public sector and critical infrastructure, and 4) empower critical infrastructure entities to identify and address threats.

*5th annual National Coordination Exercise*

## 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.** CIDR facilitates the multi-stakeholder, government-led Critical Infrastructure Cybersecurity Working Group (CICWG) that deliberates key issues and develops recommendations and priorities for strengthening the cybersecurity of specific entities and across government. Implemented in cooperation with the Ministry of Information Society and Administration, the CICWG has helped inform legal and regulatory framework, cybersecurity governance, incident-response procedures, information-sharing mechanisms, and cyber workforce development needs.

**Policy development**. CIDR advises on best practices for cybersecurity strategy and compliance so national activities meet standards set by the International Organization for Standardization (ISO) and National Institute of Standards and Technology (NIST).

**Institutionalize and expand information sharing.** CIDR is assisting the national Cyber Incident Response Team to increase the number of entities that use its platform and foster the sharing of threat and vulnerability information between and within critical infrastructure sectors.

**Accelerate cybersecurity workforce.** CIDR—with support from the UK Foreign, Commonwealth & Development Office—is developing cyber-related curricula to align academic institutions with cybersecurity market needs; CIDR is also empowering teaching staff at universities and other learning facilities with the skills to administer updated cyber curricula.

**Promote digital transformation.** CIDR assisted the government to prepare its institutions and internal processes for upcoming digital transformation activities that will strengthen service delivery to citizens and businesses and support public administration and other national priorities.

# SUB-ACTIVITIES

**CYBER PATHWAYS FOR WOMEN:** CIDR's Cyber Pathways for Women (CPW) activity is assisting the institutions of North Macedonia and employers to identify supply and demand inhibitors for women in cybersecurity careers and mitigate or remove these inhibitors. CPW is launching and will facilitate the Cyber Pathways Task Force; this strategic, multi-stakeholder group will establish dialogue between decision makers who affect cybersecurity workforce development for women. Ultimately, the task force will become a standing multi-year national program to attract more women into cybersecurity careers. CPW is being implemented as part of USAID's Women's Economic Empowerment (WEE) Initiative.

**MINISTRY OF AGRICULTURE:** CIDR is strengthening the cybersecurity posture of the ministry by using a risk-based approach to implement an information security management system, technical controls and measures, and updated and expanded cyber hygiene and resilience training. This assistance will also focus on broader adoption of security controls, technology adoption, and workforce upskilling across key government institutions to improve response capabilities in the face of a heightened threat environment in the region.