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 protect infrastructure such as energy, telecom, finance, and e-services from these malicious attacks. CIDR implements a variety of initiatives for USAID, including the Cyber Pathways for Women activity.

CYBER PATHWAYS FOR WOMEN FOCUS

Eastern Europe lacks sufficient trained personnel to protect its key institutions from cyberattacks. CIDR's Cyber Pathways for Women activity is assisting Moldova, North Macedonia, and Serbia to identify the supply and demand inhibitors for women in cybersecurity careers and mitigate or remove these inhibitors. This work is being done in support of the Women's Entrepreneurship and Economic Empowerment Act.

Photo: gorodenkoff

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 National Cyber Pathways Task Force (CPTF). These country-based task forces will convene key stakeholders within the cybersecurity workforce development ecosystem to develop activities and partnerships that will open career pathways for women.

Design gender-sensitive approaches to curriculum development. We work with universities, professional accreditation programs, and technical and vocational institutions to pilot curriculum reform training that creates gender-inclusive programs for cybersecurity professionals.

Mentor women entering the cybersecurity profession. We identify national cybersecurity professionals willing to mentor women entering the cybersecurity profession and private companies willing to hire interns, support interns, and champion graduate programs.

Initiate reform dialogue. We support public-private dialogue to help engrain gender equity and social inclusion (GESI) policies, affirmative action, and the celebration of role models.

Promote awareness. We develop social media and traditional media materials that target women and influencers in their communities. The targeting will also aim to raise awareness about cyber job and academic opportunities for women.

Empower employers. CIDR works with employers to develop the tools and procedures that enable them to grow inclusively and increase access to skilled women and other marginalized groups for hiring.

ANTICIPATED RESULTS

INFORMED LOCAL INFLUENCERS: Women, girls, and influencers in families and communities will gain access to gender-inclusive content that opens doors to cyber career paths.

WELL PREPARED WOMEN: Women will possess the knowledge and skills required to serve the cybersecurity labor market, especially in cybersecurity of critical infrastructure.

ENABLED EMPLOYERS: Private and public sector employers will obtain access to the tools and information they need to bolster their cybersecurity workforces through the integration and retention of skilled and motivated women.

SUPPORT FROM DECISION MAKERS: Key decision makers will understand and embrace the key elements needed to strengthen and diversify the cybersecurity workforce.

Photo: TommL

CONTACT: CIDR-CPW@dai.com