Critical Infrastructure Digitalization and Resilience Regional Activity

Goals

Provide assistance to improve North Macedonia's critical infrastructure, cybersecurity, and resilience.

Assist the government and critical infrastructure operators to address core cybersecurity vulnerabilities.

Duration

September 2021–September 2026

USAID Funding

$2,654,599 for activities in North Macedonia

FCDO Funding

$975,956

Implementing Partners

DAI Global, LLC in collaboration with
Policy & Management Consulting Group
SecDev and TAG International

Key Counterparts

Critical Infrastructure Operators
Critical Infrastructure Regulators
Ministry of Digital Transformation
Ministry of Agriculture, Forestry, and Water Economy
MKD-CIRT, The National Center for Computer Incidents Response
Agency for Electronic Communications

Contact

Margareta Lipkovska Atanasov
Email mlipkovska@usaid.gov

CHALLENGES

In the Western Balkans, the level of sophistication, persistence, and technical capability of cyber adversaries to attack critical infrastructure systems is on the rise. Cyber attacks against critical infrastructure and information ecosystems can diminish citizens' confidence in public institutions as well as economic operations, leading to instability and erosion of social cohesion. In North Macedonia, the government, critical infrastructure operators, and private sector face a shortage of skilled cybersecurity personnel particularly among young professionals. Compounding this shortage of trained cybersecurity professionals, many USAID partner countries in the Western Balkans lack adequate cybersecurity strategies, laws, systems, and institutions to respond to accelerating cyber threats. However, international allies including the European Union and NATO require that cybersecurity systems and structures be in place to address core vulnerabilities.

ACTIVITY DESCRIPTION

This activity assists the Government of North Macedonia in strengthening cybersecurity to protect digital information in critical infrastructure sectors including energy, telecommunications, and finance from being taken, damaged, modified, or exploited. The activity engages key stakeholders from the public, private, and civil sectors, and academia to identify national cybersecurity needs, informing government policy and decision making. Activities also include partnering with the government to draft legal and policy frameworks, address critical infrastructure challenges, promote coordinated and collaborative responses to threats, and provide capacity building initiatives for key stakeholders.

The activity further aims to create or upgrade cybersecurity curricula with academic institutions to better align with market needs. To address the shortage of skilled labor, the activity helps identify cybersecurity workforce deficiencies, provide capacity building, and supports cross-sectoral sharing of cybersecurity talent.

EXPECTED OUTCOMES

- Advanced development of legislation related to critical infrastructure law.
- Increased operationalization of national cybersecurity authorities.
- Increased cybersecurity workforces within critical infrastructure entities.
- Increased information sharing between and within critical infrastructure sectors.
- Increased capacity to address cybersecurity issues within North Macedonia's Computer Incident Response Team.

KEY RESULTS IN 2023

Cyberattack Assistance

CIDR assisted North Macedonia's Ministry of Agriculture, Forestry, and Water Economy following a major cyberattack that disabled the Ministry and its 40 branch offices; the attack disrupted the lives of 1.3 million people, many living in rural or smaller urban areas.

Compliance

The activity is working hand in hand with North Macedonia's public electricity operators to be 100% compliant with Energy Regulatory Commission cybersecurity rules.

Coordination

Hosted a cyber drill to reinforce critical infrastructure operators' resilience, security, and capacity for coordinated crisis management.

Research

Conducted research on social trends at 11 universities about social norms, employer, and academic needs that affect the uptake of women and girls into cybersecurity academic and career tracks.

ACCOMPLISHMENTS

The Cybersecurity Pathways for Women component trained and introduced **cybersecurity career options** to **155 women** and **girls.**

Three Train the Trainers courses educated **83 university** teaching **staff** and **Training Providers** on IoT Security and Privacy, Cyber-Physical Systems Security of Critical Infrastructure, and Digital Forensics.

The Critical Infrastructure Cybersecurity Working Group held **17 working sessions** where the group identified **8 critical infrastructure sectors** for North Macedonia. Three sectors were selected as priority for cataloging: **energy**, **finance** and **telecom**.