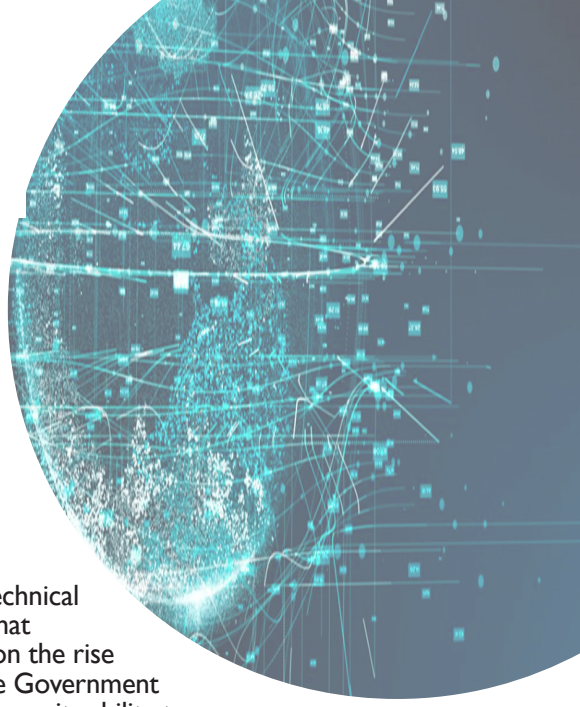
USAID
FROM THE AMERICAN PEOPLE

UK International Development
Partnership | Progress | Prosperity



REGIONAL ACTIVITY
CRITICAL INFRASTRUCTURE DIGITALIZATION AND RESILIENCE

Goals

Provide assistance that helps North Macedonia improve its critical infrastructure cybersecurity and resilience

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

Duration

September 2021– September 2026

USAID Funding

$1,865,262 for activities in North Macedonia

FCDO Funding

$975,956

Implementing Partner

DAI Global, LLC

In collaboration with:
- TAG International
- SecDev
- Florida International University
- Policy & Management Consulting Group

USAID Contact

Margareta Lipkovska Atanasov
mlipkovska@usaid.gov

FCDO Contact

Liljana Ristovska
Liljana.Ristovska@fcdo.gov.uk

BACKGROUND

Cyber adversaries' level of sophistication, persistence, and technical capability to attack the systems that support critical infrastructure is on the rise in Western Balkans countries. The Government of North Macedonia aims to improve its ability to protect infrastructure such as energy, telecommunications, and e-services and ensure that systems and structures are in place to meet the future requirements of international allies such as the European Union and NATO.

North Macedonia adopted its National Cybersecurity Strategy in 2018. As of 2023, the Ministry of Information Society and Administration is significantly revising the strategy to make it more applicable. Also in 2022, North Macedonia drafted a new Critical Infrastructure Law that aims to define critical physical infrastructure sectors that must be protected.

Additionally, the government, infrastructure operators, and private sector face a shortage of skilled cybersecurity personnel due to outdated education system and teaching methodologies, non-standardized cybersecurity job descriptions and qualifications, and a significant brain drain to other countries, particularly among young professionals.

In 2021, USAID supported a pilot program in North Macedonia that identified priority areas for engaging in cybersecurity to protect digital information from being taken, damaged, modified, or exploited. The pilot also helped establish a Critical Infrastructure Cybersecurity Working Group—comprised of key stakeholders from North Macedonia's public, private, and civil sectors, and academia—to deliberate on national cybersecurity needs and inform government policy and decision making.

PROGRAM DESCRIPTION

Through the Critical Infrastructure Digitalization and Resilience regional activity, USAID is supporting the Government of North Macedonia to finalize the legal framework for the National Cybersecurity Strategy. We are partnering with the government to draft legal and policy frameworks, address critical infrastructure challenges such as threat identification and information sharing, and provide capacity building initiatives for key stakeholders.

USAID has also led collaboration between the British Embassy Skopje Foreign, Commonwealth & Development Office (FCDO), the Government of North Macedonia, and the private sector to build the country's cybersecurity workforce through this Activity. Continued partnership between the U.S., UK, and North Macedonia aims to improve domestic capacity to advance regional stability and security in cyberspace.

To address the shortage of skilled labor, we will identify cybersecurity workforce deficiencies and provide capacity building; create a public/private sector mechanism to facilitate cross-sectoral sharing of cybersecurity talent; and create better market-aligned cybersecurity curricula with academic institutions.

We will also support the establishment and use of information-sharing networks between national and regional critical infrastructure entities, promoting coordinated and collaborative responses to threats.

EXPECTED RESULTS AND IMPACT

- The Ministry of Information Society and Administration will be better able to sustainably administer and use the Critical Infrastructure Cybersecurity Working Group to create and operationalize national competent authorities, mobilize sector Computer Security Incident Response Teams (C-SIRTs), advance the development of primary and secondary legislation, and support institutions charged with overseeing implementation of new Critical Infrastructure Law to draft sub-laws.

- Cybersecurity workforce deficiencies of targeted critical infrastructure entities will be identified and addressed.

- The capacities of North Macedonia's computer incidence response team (MKD-CIRT) will be strengthened.

- The Government of North Macedonia and operators will expand the national information-sharing platform to increase the number of entities that use the platform and foster the sharing of threat and vulnerability information between and within critical infrastructure sectors.