CYBERSECURITY

OVERVIEW

Cyber is a critical frontline as Ukraine defends its security, independence, and democracy from Russia's aggression. In recent years, USAID has made major investments in Ukraine's ability to respond and recover from cyberattacks emanating from Russia, including attacks targeting the Government of Ukraine and critical infrastructure operators. USAID cybersecurity assistance is part of our overall effort to strengthen Ukraine's resilience to Russia's aggression and to promote economic growth and effective democratic governance. Our programming strengthens the capacity of Government of Ukraine agencies, ministries, and parliamentary committees; helps secure democratic elections; and raises awareness among civil society, the private sector, and the general public about the importance of cybersecurity. Since Russia launched its full-scale invasion of Ukraine in February 2022, we have expanded our programming to protect public communications networks by repelling cyberattacks and repairing systems following attacks, as well as by ensuring continued voice and data connectivity.

PROGRAM OBJECTIVE

To enhance Ukraine's overall security by strengthening its ability to prevent and mitigate cyberattacks, and to quickly recover and restore critical infrastructure after an attack has occurred.

OUR PROGRAMS

CYBERSECURITY FOR CRITICAL INFRASTRUCTURE IN UKRAINE

USAID launched the four-year, $38 million Cybersecurity for Critical Infrastructure in Ukraine activity in May 2020 and to strengthen Ukraine's cyber preparedness and protect critical infrastructure through assistance in three key directions: 1) strengthening the cybersecurity enabling environment; 2) developing Ukraine's cybersecurity workforce; and 3) building a resilient cybersecurity industry. The activity improves cybersecurity products and services through increased public-private sector collaboration and expands market opportunities for Ukrainian cybersecurity firms by opening access to capital and new local and international markets. The activity has a strong component to build the cyber resilience of Ukraine's energy sector. Under the activity, participating electricity utilities are developing five- and ten-year network development plans and receiving training on how to improve organizational structure,

operations, and procurement standards. Participating energy regulatory agencies are developing strategies to address energy sector cybersecurity, and are receiving training on cyber-hardened electricity network upgrades. They are also facilitating dialogue between utilities and regulators to ensure that appropriate upgrades are made to the network in a financially sound manner.

Following Russia's full-scale invasion of Ukraine, the activity funded technical experts to provide hands-on support to essential service providers within the Ukrainian government including government ministries and critical infrastructure operators to identify malware and restore systems after an incident has occurred. This support builds on long standing USAID support building cyber resilience among regional utilities, particularly in the energy sector. Amid Russia's invasion, USAID has also provided more than 6,750 emergency communications devices, including satellite phones and data terminals, to essential service providers, government officials, and critical infrastructure operators in key sectors such as energy and telecommunications.

UKRAINE RESPONSIVE AND ACCOUNTABLE GOVERNANCE PROGRAM

In 2016, USAID launched the nine-year, $81 million Ukraine Responsive and Accountable Governance Program to promote citizen-centered elections and political processes in Ukraine. Under the activity's cybersecurity component, USAID partners with Ukraine's Central Elections Commission (CEC) to strengthen its cybersecurity capacity and counter growing online threats to electoral systems. The activity conducted an electoral cybersecurity needs assessment and worked with key elections and cybersecurity actors to provide critical improvements to electoral cybersecurity infrastructure. URAP conducted cyber hygiene training for election commissioners at all levels, as well as for civil society, political parties, and the Parliament, training 642 individuals nationwide in 2019. In doing so, the activity developed and conducted cybersecurity training courses for IT professionals in Ukraine and beyond. The activity strengthened the cybersecurity resilience of Ukraine's electoral results management system and voter registry, enabling Ukraine's Central Election Commission to combat cyberattacks during the country's 2019 presidential and snap parliamentary elections – safeguarding confidence in electoral processes.

USAID/WASHINGTON AND REGIONAL PROGRAMS

REGIONAL ENERGY SECTOR CYBERSECURITY ACTIVITY

The United States Energy Association and the National Association of Regulatory Utility Commissioners are cooperating to improve energy-sector cybersecurity. This $1 million regional program is working to establish mechanisms for sharing knowledge and best practices across energy sector entities in Ukraine, Moldova, Armenia, and Georgia, focusing on strengthening cybersecurity capabilities among energy sector regulators and electricity transmission and distribution companies.