Memorandum of Understanding

Between the Ministry of Foreign Affairs of Ukraine and DAI Global LLC

Kyiv, 24.05, 2022

The Ministry of Foreign Affairs of Ukraine, as Recipient, and DAI Global LLC (DAI), as Implementer, of the United States Agency for International Development (USAID) Cybersecurity for Critical Infrastructure in Ukraine Activity (the "Project"), hereinafter collectively referred to as the "Parties", hereby affirm, by entering into this Memorandum of Understanding (MOU), their intend to cooperate within the Project objectives, tasks, and expected results included below.

1. Project goal and objectives

The Project is funded by USAID and implemented by DAI. The purpose of the Project is to strengthen the resilience of Ukraine's critical infrastructure from cyberattacks by establishing trusted collaboration between key cybersecurity stakeholders in the government, private sector, academia, and civil society. To achieve this goal, the Project will pursue the following objectives:

- **Strengthen the cybersecurity enabling environment:** Strengthen the legal, regulatory, and institutional framework for national cybersecurity in Ukraine to increase preparedness and resilience based on international standards and best practices.
- **Develop Ukraine's cybersecurity workforce:** Address workforce gaps to develop new cybersecurity talent and build the capacity of existing cybersecurity professionals.
- **Build a resilient cybersecurity industry:** Build trust and collaboration between the public and private sectors to respond more effectively to cybersecurity challenges and support the growth of a broader cybersecurity market in Ukraine.

2. Term of assistance

From _____ to September 17, 2024.

3. Project tasks

The Project is organized into three components aligned with the primary objectives described above.

COMPONENT 1: Strengthen the cybersecurity enabling environment

This component will strengthen the cybersecurity resilience of Ukraine's critical infrastructure sectors by addressing legislative gaps, promoting good governance, enabling collaboration between stakeholders, and supporting cybersecurity institutions. This component will also build the technical capacity of key sectors through increased access to cybersecurity technology and equipment.

COMPONENT 2: Develop Ukraine's cybersecurity workforce

This component will increase capability and capacity along the entire workforce pipeline through activities focused on education received by cybersecurity specialists and industry training programs to rapidly upskill the workforce to respond to immediate cybersecurity vulnerabilities and prepare for future challenges.

COMPONENT 3: Build a resilient cybersecurity industry

This component will facilitate public-private collaboration to increase innovation in cybersecurity solutions; support smaller cybersecurity companies to rapidly increase the number of local cybersecurity service providers; increase access for finance for viable cybersecurity providers; and offer mechanisms for Ukrainian firms to connect with industry partners to enable better access to business opportunities.

Support to the recipient, as described below, will primarily fall under Component 1 and will provide them with targeted assistance to cybersecurity activities based on their most pressing needs.

Expected results of the Project's implementation (specific to the recipient)

Through technical assistance and the provision of cyber security technology, the recipient will be better positioned to deter and respond to cyberattacks, including those resembling attacks that have knocked down government websites.

4. Quantitative and/or qualitative criteria of achieving the Project effectiveness

The Project will put in place a robust monitoring and evaluation system to measure results and guide Project activities, and work plan development. Key indicators include:

- Improved cybersecurity capacity through USG-assistance (provision technology and technical assistance)
- Improved ability to deter, detect, and respond to cybersecurity attacks
- Uptake of new technology

5. Lists of assets, works and services, intellectual property rights, other resources to be purchased and provided under the Project

- Needs assessment
- IT/cybersecurity equipment and software
- Technical assistance/expertise
- Training

6. Expected impact of the Project on the development of the economy and region

Results and outcomes from the Project will improve short-term cybersecurity resilience in Ukraine and establish a solid foundation for long-term cybersecurity independence and leadership. Lessons learned and best practices from the improved cybersecurity of key critical infrastructure sectors will be extended to other public sectors, as well as to the private sector and civil society.

7. Commitments of the Implementer regarding assistance

Subject to the availability of funds, DAI intends to:

- Support the Ministry of Foreign Affairs of Ukraine's efforts to:
    - Bolster its cybersecurity systems
    - Bolster its cybersecurity processes through technical assistance/expertise
    - Improve/increase the skills of their cybersecurity professionals

All undertakings of DAI pursuant to this MOU are subject to the availability of funds. This MOU is not intended to affect funding obligations on the part of USAID.

8. Obligations of the Recipient

The Ministry of Foreign Affairs of Ukraine intends to:

- Designate a primary point of contact to facilitate communication and coordination.
- Provide the Implementer with appropriate information as required to support assistance efforts and report on implementation.
- Provide data to the Implementer for measuring impact.
- Track and report on assistance provided by the Implementer.

This MOU takes effect on the day of its signing and will be effective until September 17, 2024

The Ministry of Foreign Affairs of Ukraine

Olersandr Bankov
State of Foreign Affairs of Ukraine

Date: 24.05.2022

DAI Global LLC, USAID Cybersecurity for Critical Infrastructure in Ukraine Activity

Petro Matiaszek
Chief of Party, DAI Global LLC

Date: 24.05.2022