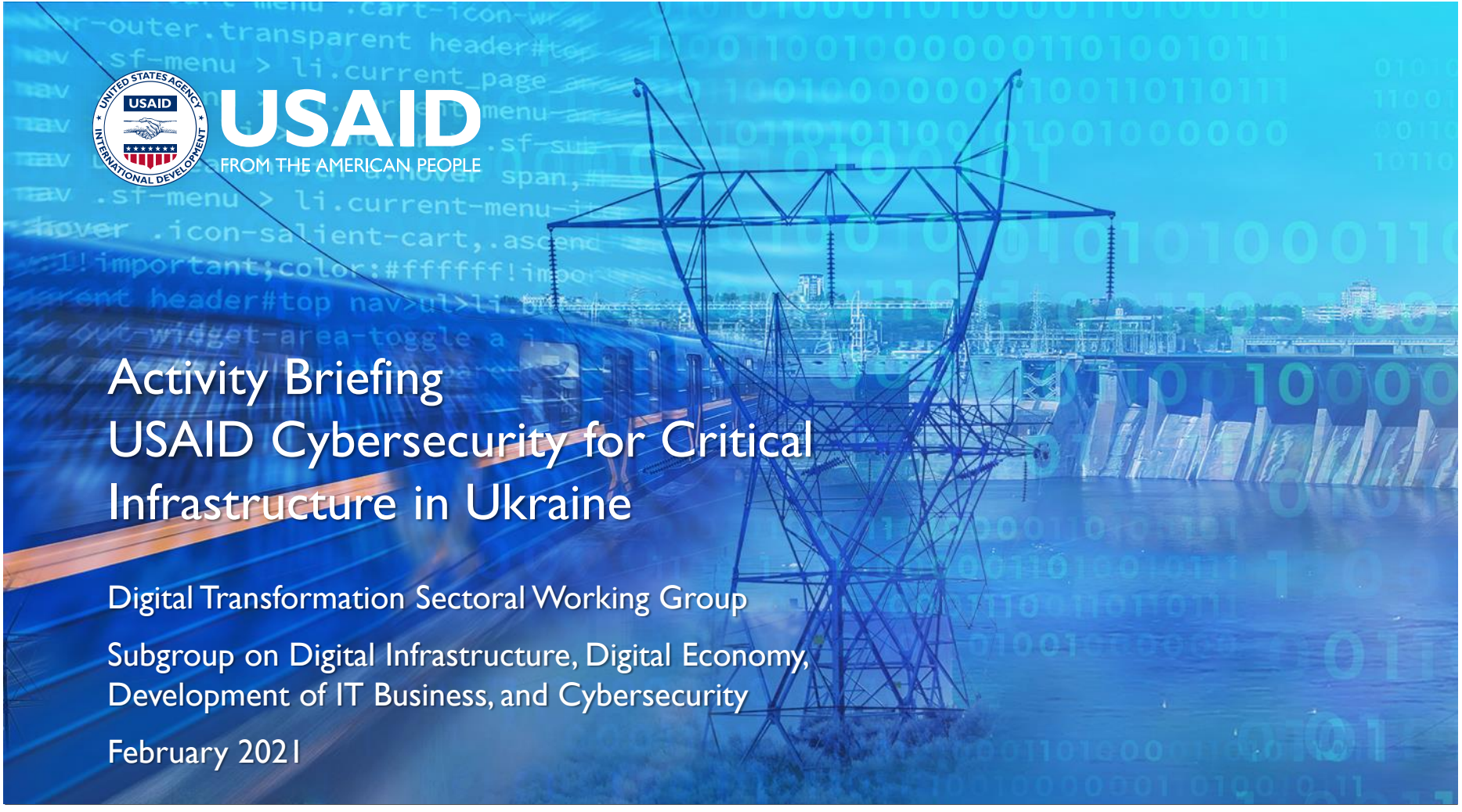

Activity Briefing
USAID Cybersecurity for Critical Infrastructure in Ukraine

Digital Transformation Sectoral Working Group

Subgroup on Digital Infrastructure, Digital Economy, Development of IT Business, and Cybersecurity

February 2021

ACTIVITY SUMMARY: USAID CYBERSECURITY for CRITICAL INFRASTRUCTURE

FUNDED BY:

U.S. Agency for International Development

IMPLEMENTED BY:

DAI with partners

ACTIVITY DURATION:

May 2020 – September 2024

ACTIVITY GOAL:

Reduce cybersecurity vulnerabilities in critical infrastructure and transform Ukraine into a resilient, agile cybersecurity leader.

OVERVIEW OF ACTIVITY

USAID Cybersecurity has three main components aligned to strategic objectives:

PROJECT COMPONENTS

STRENGTHEN UKRAINE'S CYBERSECURITY ENABLING ENVIRONMENT

DEVELOP UKRAINE'S CYBERSECURITY WORKFORCE

BUILD A RESILIENT CYBERSECURITY INDUSTRY

STRATEGIC OBJECTIVES

Create a safe and trusted environment to accelerate the development of people, processes, and technology in support of critical infrastructure cybersecurity.

Strengthen Ukraine as a sovereign nation built on a secure, protected, and dynamic economy, supported by a talented pool of human capital.

Stimulate demand and supply for cybersecurity solutions and service providers to empower, equip, and finance Ukrainian cyber entrepreneurs.

TASKS BY COMPONENT

ENABLING ENVIRONMENT

- Legal and governance environment aligned to international norms and standards
  - National strategy and roadmap
  - Legislation, institutional and governance reforms
- Greater coordination among public and private sector stakeholders
- Ad hoc assistance for expertise and technical needs
- National preparedness and resiliency:
  - Increased threat intelligence sharing
  - Public sector capacity building
  - Improved cybersecurity at operator level
  - National preparedness exercises

WORKFORCE DEVELOPMENT

- Increased capacity to generate cybersecurity graduates at university level
  - Instructor training and cybersecurity training labs
- Increased number of skilled cybersecurity professionals
  - International certification and customized training courses
  - Capacity building in stakeholders
  - Peer mentorship program
- Increased awareness of cybersecurity practices among workers
  - Cyber hygiene

MARKET DEVELOPMENT

- Innovation and partnerships to drive effective solutions
  - Center for Cyber Innovation
  - Demonstrate PPP models
- Increased investment in cybersecurity sector
  - Promote and facilitate investments and partnership
- Growth opportunities for small and medium cybersecurity providers
  - Small and Medium Business Acceleration and Mentorship
  - Market information exchange platform

UKRAINIAN STAKEHOLDERS

KEY STAKEHOLDERS/ BENEFICIARIES

Ministry of Digital Transformation (MDT)

National Security and Defense Council (NSDC)

State Service for Special Communications and Information Protection (SSSCIP)

ADDITIONAL STAKEHOLDERS

Verkhovna Rada
(Committee on Digital Transformation; others as appropriate)

Specific Ministries
(Energy; Infrastructure; Economic Development, Trade and Agriculture; Strategic Industries of Ukraine)

Private Sector
(Business and professional associations; IT sector companies)

Academia
(Public and private universities)

Expert Council on Cyber and Information Security

Accomplishments and Ongoing Assistance

- Digital transformation security: DIIA Mobile App penetration testing and Bug Bounty program
- Critical infrastructure cybersecurity: cyber diagnostics and training in selected critical infrastructure operators
- Organizational/Technical models and solutions: Initial models for improved threat information sharing and development of the registry for Critical Information Infrastructure (CII)
- Governance and multi-stakeholder input: support to the Expert Council on Cyber and Information Security, roundtable on development of national strategy
- Organizational capacity: communications support, organizational audits, training
- Workforce Development: Higher Education Roundtable and solicitation of applications for program participation
- Baseline assessments (enabling environment, preparedness, workforce development, market)

KEY OBJECTIVES and WORKSTREAMS FOR 2021

- ❑ Development of the new National Cybersecurity Strategy
- ❑ Development of a Cybersecurity Roadmap
- ❑ Institutional and governance reforms
- ❑ Drafting supporting legislation and policies
- ❑ Introduction of international best practices: frameworks, standards, directives
- ❑ Threat intelligence sharing pilot program
- ❑ CII registry implementation
- ❑ Launch of private sector programs: Business acceleration and mentorship
- ❑ Higher Education Program – instructor training and cybersecurity training labs
- ❑ Cybersecurity audits and development of a Cyber Maturity Model
- ❑ Cybersecurity professional training program
- ❑ Center for Cyber Innovation
- ❑ Industrial Control Systems Lab
- ❑ National Preparedness (Tabletop) Exercise

USAID
FROM THE AMERICAN PEOPLE

Thank you!
Дякую!

Contact:

Tim Dubel
Chief of Party
timothy_dubel@DAI.com