INVITATION

TO THE

Pilot Course on Critical Infrastructure Protection

Module 2 — From Risk Management to Resilience

(ESDC Activity Number 2020-21/255-2/1)

Online, 23-25 February 2021

The Joint Research Centre (DG JRC), the Digital Security Authority (DSA) - National CSIRT-CY of Cyprus and the National Institute of Research and Development in Informatics (ICI Bucharest, Romania) have the great honour of organising jointly the second Module of the Course on Critical Infrastructure Protection - From Risk Management to Resilience. This module is part of the training activity of the European Security and Defence College (ESDC) on "Critical Infrastructure Protection". The first pilot module was organized by ICI Bucharest under the aegis of the European Union External Action's (EEAS) European Security and Defence College (ESDC) and with the support of the Joint Research Centre of the European Commission.

This second module will cover the topics of Cyber, Transport, Energy and Space and their interdependencies. It will be structured around a number of presentations, breakout working groups and a tabletop exercise. Considering the implications of the ongoing COVID-19 pandemic, the course will be organized between 23 and 25 February 2021 through online seminars as well as uploaded contributions on the ESDC's ILIAS platform, including additional pre-recorded lectures.

The course aims to provide a forum for the exchange of knowledge and best practices among experts whose working areas are related to the protection of Critical Infrastructure by improving their knowledge, skills and competences and offering them tactical/operational-level training. This is a specialized course and therefore participants should be familiar with the basic terminology and concepts. Graduates of Module 1 are welcome to attend and will have the most to gain from this continuous educational approach.

This training activity is open to civil servants and military personnel from EU Member States, EU institutions and agencies who are currently employed in positions relevant to the topics of this course. The course is particularly relevant for those dealing with cyber operational / tactical topics related to the protection of Critical Infrastructure and Critical Information Infrastructure or who are willing to discuss and update their knowledge on these issues. The participants of the first module have the highest priority to follow this module.

Dan Claudiu CHIRONDOJAN
Director
European Commission
DG Joint Research Centre
Directorate E – Space, Security and Migration

Adrian-Victor VEVERA
General Director
National Institute for Research and Development in Informatics ICI Bucharest

Antonis ANTONIADES
Director
Digital Security Authority of Cyprus

Annex 1 : Audience and Learning outcomes

Target Audience:

- Mid to high level representatives of public authorities or CI owners/operators (private and governmental) with responsibilities for the formulation and implementation of security strategies and mechanisms for Critical Infrastructure Protection;
- Participants will be from the EC, from National governments of EU Member States and from state and private companies involved in CI operation.

The table below summarizes the learning outcomes from this course:

Learning outcomes	Knowledge	○ Increase the understanding of CI interdependencies; ○ Assimilate new knowledge on CI sectors such as Energy, Transport, Cyber and Space; ○ Recognize the new realities of the complex security environment; ○ Update the knowledge on Critical Infrastructure Protection framework at European level in accordance with the new documents of reference published by the European Commission in December 2020; ○ Understand the emerging trends producing new risks, vulnerabilities and threats; ○ Improve the participants' understanding of the toolbox available to CIP practitioners and policymakers; ○ Understand emerging areas of CIP focus, such as space and global dimensions.
	Skills	○ Identify technical, organizational and transborder coordination challenges related to CIP; ○ Consider the potential systemic impact of European and global integration on CIP governance efforts; ○ Consider the impact of new technologies (such as trusted AI) and new priorities (such as climate change) on public policy related to CIP; ○ Identify the challenges for policymakers, regulators and CIP practitioners stemming from the changing security environment.
	Competencies	○ Evaluate the potential impact of new technologies and other trends on CI system-of-systems risks; ○ Assess the challenges to CIP efforts at National and European levels moving forward given the new security environment; ○ Use a systemic and complex understanding of the security environment, grounded in the CIP framework and its latest developments; ○ Systematize complex systems from a CIP perspective in order to address security issues utilizing the CIP framework.

Some of the topics to be addressed in the course:

- The evolution of the security environment;
- The new dimension of hybrid threats;
- Toolsets and technologies for CIP;
- Sectoral aspects of CIP – Cyber, Transport, Energy and Space;
- Decision-making for crisis and emergency situation management.