

# First IEEE International Workshop on Critical Infrastructure Protection

November 3 – 4, 2005 — Darmstadt, Germany  
<http://www.iwcip.org/2005/>

## Important Dates

Full paper submissions due: **June 17, 2005**  
Notification of acceptance: July 15, 2005  
Final papers due: August 5, 2005  
Workshop: November 3 – 4, 2005

## Background

The protection of critical infrastructures such as telecommunications, energy, financial services, health care, public services, and transportation has moved from being primarily driven by safety and engineering concerns to also incorporating elements of security, particularly from external hostile actions, but also including sabotage from within. Moreover, these critical infrastructures not only exhibit strong interdependence but are also increasingly relying on information systems for their operation.

The large number of cross-cutting concerns at both technical and organizational levels require interdisciplinary research and collaboration in a number of areas including information assurance, control systems, and power engineering at the technical level and also require consultation and coordination at both domestic and international policy levels.

## Overview

The IEEE Task Force on Information Assurance is sponsoring an interdisciplinary workshop on research, policy, and experience in the field of critical infrastructure protection (CIP) and critical information infrastructure protection (CIIP).

The workshop seeks submissions from academia, government, and industry presenting novel research, policy, and applications and experience in the field of critical infrastructure protection. Possible topics include, but are not limited to the following:

### *Scientific and Technical Understanding of CIP/CIIP*

- Modeling, analysis, and assessment of infrastructures and their interdependencies
- Identification of public and private assets for CIP/CIIP

- Analysis and management of threats, risks, and vulnerabilities of critical infrastructures at the national level
- Cyberterrorism, cybercrime, and information operations

### *Scientific, Technical, and Organizational Approaches for CIP/CIIP*

- Information security, security engineering, software security for CIP/CIIP
- CIP/CIIP requirements of the information society
- Early warning and information sharing networks
- Knowledge-based alerting and management approaches and mechanisms
- Public-Private-Partnerships (PPP) and their security requirements for cooperative CIP/CIIP
- Information Sharing and Analysis Centers (ISAC), information sanitization, and secure exchange of confidential information
- Global/enterprise security architectures and information infrastructures

### *National and Transnational CIP/CIIP Positions and Issues*

- Definition and analysis of national CIP/CIIP policies and positions
- Mechanisms for international cooperation among CIP groups

Accepted papers will be published by IEEE Computer Society Press.

## Program Committee

Eyal Adar (IT-CON, Israel)  
Jack Cole (US Army Research Laboratory, USA)  
Geert Deconick (K.U. Leuven, Belgium)  
Dorothy Denning (US Naval Postgraduate School, USA)  
Myriam Dunn (ETH Zürich, Switzerland)  
John James (United States Military Academy, USA)  
Stephan Lechner (Siemens, Germany)  
Eric Luijff (TNO FEL, The Netherlands)  
Götz Neuneck (U. of Hamburg, Germany)  
Lars Nicander (FHS Stockholm, Sweden)  
Saifur Rahman (Virginia Tech, USA)

## General Chair

Bernhard Hämmerli (HTA Lucerne, Switzerland)

## Program Chair

Stephen D. Wolthusen (Fraunhofer-IGD, Germany)

## Full Paper Submission Guidance

Submissions must not substantially duplicate work that any of the authors has published elsewhere or has submitted in parallel to any other conference or workshop with proceedings. The paper must list all authors and their affiliates on a separate sheet; in case of multiple authors, the contact author must be indicated. The paper itself must be blinded. It should begin with

a title, a short abstract, and a list of key words, and its introduction should summarize the contributions of the paper at a level appropriate for a non-specialist reader. Submissions should have at most 10 pages excluding the bibliography and appendices (using 10pt body text and two-column layout), and at most 15 pages total. Submissions not meeting these guidelines risk rejection without consideration of their merits.

Submissions and questions should be sent electronically to [SWOLTHUSEN@IEEE.ORG](mailto:SWOLTHUSEN@IEEE.ORG).

## Additional Information

Additional information on the workshop and related events can be obtained from

<http://www.iwcip.org/2005>

The workshop will be held cooperation with the special interest group on critical infrastructure protection (FG KRITIS) of the Gesellschaft für Informatik

