Information Technology has become pervasive in all aspects of our lives and increasingly is involved in critical infrastructures. This minitrack examines aspects associated with the security of information technology and critical infrastructures (with an emphasis on automated control systems) and explores ways that IT can enhance the ability of governments to ensure the safety and security of its citizens. Governments have also embraced IT to interface with citizens in a more efficient manner. Security issues have risen to the forefront as a result of data disclosures and identity theft incidents discussed in mainstream media. Other issues governments are dealing with include intellectual property theft and criminal acts involving computers. Although 85% of the US critical infrastructure components are privately owned and operated, government has a seat at the table, as security is one of the regulatory issues under government purview. Control system networks, including the operation technology (OT) networks that manage our critical infrastructures, have evolved into Internet connectable structures. For this reason, this minitrack has begun to look at the importance of industrial control systems (ICS) security as related to government operations. Sometimes referred to as cyber-physical systems or supervisory control and data acquisition systems (SCADA), these systems have a profound impact on governments and the people they serve.

This year’s submissions cover a broad spectrum of security topics. We are especially pleased with the international participation in the minitrack. Five papers have been chosen from a wide selection of submissions. These presentations are grouped into two sessions. We express our sincere appreciation to those authors that took the time to submit a paper for our consideration and our congratulations to those that were accepted.

The first session presents three papers, beginning with Designing a Formal Model Facilitating Collaborative Information Sharing for Community Cyber Security was authored by Zhao and White, proposes a group-centric collaborative information sharing framework that aims to improve community cyber security. The next paper, Security Analysis of Selected AMI Failure Scenarios Using Agent Based Game Theoretic Simulation reports on leading edge research at Oak Ridge National Laboratory which presents a game theoretic examination of failure scenarios in AMI networks, a key element of SmartGrid deployments. The final paper of the first session is Municipal E-Government Security: Insights from a Study of Orange County, California, authored by Timothy Perez, presents an examination of the adequacy of e-government security at a municipal level.

The second session has two papers, Reengineering Cybersecurity Education: An Analysis of the Critical Factors, from the University of Houston, presents a look at the critical success factors in designing critical infrastructure security education, followed by Unintentional Insider Threat: Contributing Factors, Observables, and Mitigation Strategies, a paper from research at the Software Engineering Institute at Carnegie Mellon University, which examines the issues associated with insiders that unintentionally perform actions that expose the organization to increased risk.

We sincerely hope that the attendees enjoy this session and will contribute to the discussion we are certain that occur following the paper presentations.