# Introduction to the Security and Privacy in Government Minitrack

Gregory B. White
UT - San Antonio
greg.white@utsa.edu

Wm. Arthur Conklin
College of Technology
University of Houston
waconklin@uh.edu

Keith Harrison
UT-San Antonio
keith.harrison@utsa.edu

This minitrack explores the pressing issues surrounding the intersection of cybersecurity and government spheres of influence. Whether technical or policy, from information sharing to new analytical methods for detecting threats, this mini-track casts a wide net to cross disciplinary thinking to problems with far-reaching implications. The cybersecurity aspects of critical infrastructure systems have become a hot topic for countries across the globe. Information Technology has become pervasive in all aspects of our lives, and this includes elements referred to as the critical infrastructures.

The mini-track examines aspects associated with the security of information technology (IT) and operational technology (OT) and explores ways that IT can enhance the ability of governments to ensure the safety and security of its citizens. As governments have embraced IT to interface with citizens in a more efficient manner, security issues have risen to the forefront with the data disclosures and identity theft incidents that have occurred. Other critical issues include intellectual property theft and criminal acts involving computers. Additionally, information security is an area where policy has not kept up with technology, placing nations and their relations over this topic into uncharted territories.

This year's submissions cover a broad spectrum of security topics. Four papers were chosen this year. We express our sincere appreciation to those authors that submitted a paper for our consideration and offer our congratulations to those that were accepted.

The first paper, *"Out with the Old, In with the New: Examining National Cybersecurity Strategy Changes over Time"* by W. Alec Cram and Jonathan Yuan, examines multiple NCS versions in Canada, the United Kingdom, and Australia using a qualitative, content analysis approach. The results point to four core themes that characterize NCS stability and change over time. Based on the observations, the authors articulate several theoretical propositions and outline a plan for future research.

The second paper by Natalie Sjelin and Glenn Dietrich "*Method to Identify High Value Assets for Small Government Agencies and Small- to Mid-sized Organizations*" describes a method for identifying high value assets that can be integrated into an organization's or agency's cybersecurity program. Resources that can be dedicated to cybersecurity are finite and need to be applied strategically on the most important assets in the organization.

The third paper *"The Dark Blue CyberPatriot Training Tool"* by Scott Semian and Keith Harrison, discusses a training tool to help better prepare teams for the CyberPatriot competition. This competition, sponsored by the Air Force Association, annually hosts between 5 and 7 thousand high school and middle school teams. It aims to introduce students in these grades to the field of cybersecurity.

The final paper, "*Is a Significant Demographic Left Out of the Equation? An Overview of Possible Inequitable Access to Cybersecurity Educational Programs in the United States*" by Johanna Jacob and Greg White, examines what appears to be a significant gap in access to cybersecurity programs in Title 1 and rural schools. Initial results have shown the existence of what has been described as "cyber deserts" in major areas of the nation which impacts the ability to insure equitable access to cybersecurity information for all segments of the population.

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

URI: https://hdl.handle.net/10125/79614
978-0-9981331-5-7