Press Release

The Internet of Things Security Institute (IoTSI) announced today that it has released an IoT Security Framework for Smart Cities and Critical Infrastructure.

Alan Mihalic President of the IoT Security Institute says the objective of the IoTSI is to provide the cyber and privacy frameworks that can be implemented from the base build through to the build completion.

“The goal of the IoT security Institute is to establish a comprehensive set of guidelines to help each of the supply chain participants specify, procure, install, integrate, operate and maintain IoT securely in Buildings, Smart Precincts and Cities. This includes intelligent buildings equipment and controls such as audio visual (AV), fire, HVAC, lighting and building security.

“Buildings are working spaces, information portals and community information exchanges that require appropriate security controls to meet their future potential. The IoT Security Institute is focused on ensuring that recommendations produced are globally applicable and simple to adopt – fitting within existing processes wherever possible. To achieve this, the IoTSI opens the channels of communication between building occupiers, facilities managers, engineers, designers and urban planners in relation to the cyber security and privacy challenges affecting building environments.”

In a Smart Cities age, this includes maintaining data confidentiality, privacy and public safety levels that meet community and corporate expectations. This can only be achieved by a globally available Cyber Smart Cities and Critical Infrastructure Framework.

The release of the IoTSI Framework provides business, government and industry a publically available framework capable of addressing emerging and existing IoT security challenges within the built environment. Released under a Common Criteria licensing agreement the IoTSI framework can be implemented without licensing costs or additional charges.

“We did not want to restrict framework adoption by imposing licensing costs or restricted access pending some kind of commercial consideration. The framework is there to be implemented and shared. Often the benefits of such initiatives get lost in the commercial requirements imposed. The IoTSI does not even charge membership dues. We did not want to be caught up in forcing membership on order to participate. It too often drives many Not- For-Profit agendas. We simply and easily want to get the framework to cyber and privacy professionals where it is needed”. says Alan Mihalic (left)

“Of course, there’ll be organizations that will provide professional services to assist with the Framework’s deployment. This is expected. Resource and competency considerations are always a determining factor to any cyber security or privacy process improvement activity. However, the Framework is not a commercial offering. That in itself goes a long way to keeping costs in check. Mihalic added.”

David Watts, Professor of Information Law and Policy at Latrobe University, former Victorian Privacy Commissioner and current member of the United Nations Global Pulse offered the following insight on emerging challenges facing IoT and how the IoT Security Institute is addressing those security challenges:

“The internet of things can enrich our lives and our societies but it’s vital that the risks it can pose to our fundamental freedoms are avoided. One of the key risks is security. Getting IoT privacy, security and ethics right from the outset is part of the important work that the IoTSI is undertaking through its ongoing program to develop a security framework for the [deployment of] IoT [technologies]. Crucially, this work is being developed through the efforts of organisations and individuals who are contributing a wide range of policy, technical, legal and consumer perspectives.”

About the Internet of Things Security Institute (IoTSI)

The Internet of Things Security Institute is a Not for Profit academic and industry body dedicated to providing frameworks and supporting educational services to assist in managing security within an Internet of Things eco-system. The IoTSI has developed an IoT Security Framework for Smart Cities and Critical Infrastructure, which will enable and facilitate the secure and safe deployment of IoT & IIOT Eco-Systems.

IoTSI is now inviting those with a specific interest in ensuring the safety and security of smart buildings and critical infrastructure, to get involved and help ensure the ongoing aims of the IoTSI are achieved. Interested parties can make direct contact by emailing; admin@iotsecurityinstitute.com

The IoT Security Institute Smart Cities and Critical Infrastructure Framework can be downloaded, and used for free from https://iotsecurityinstitute.com/iotsec/index.php/artefacts

For more information, news and further announcements, visit the official website at www.iotsecurityinstitute.com

--ENDS--