End to End Trust and Security Workshop
for the Internet of Things (IoT)
February 4, 2016 – George Washington University, Washington, DC

The goal of this workshop is for researchers, IT architects and security professionals from industry, government and academia to discuss and agree to the scope of an end to end trust and security open architecture for IoT, resulting in a report out and point of view on the research challenges, with recommended next steps.

Target audience is 100 to 150 attendees representing:

- Universities including researchers, IT, IoT, CISO
- Agencies including NSF, DOE, DHS, NIST, OSTP
- IoT and Standards Organizations including IEEE and IIC
- U.S. Regional Research & Education Network (e.g., NYSERNET)
- Industry leaders in IOT
- Internet2 staff and E2ET&S and IoT innovation working groups

Pre-work: A call for presentations to deliver during the workshop was issued on December 17, 2015, with submissions January 4-15, 2016.

Agenda:

8:00am	Coffee
8:30am	Welcome and introductions – Led by Oleg Logvinov, IEEE
9:00am	Opening Panel re: needs and challenges in end to end trust, security, privacy for the IoT – moderated by Florence Hudson, Internet2 ▪ Rosio Alvarez, US Department of Energy ▪ Oleg Logvinov, IEEE ▪ Bob Martin, IIC ▪ Anita Nikolich, NSF ▪ Additional participants
9:45am	Break
10:00am	Presentations from submissions on Requirements of what we need to do for E2ET&S for IoT
11:15am	Presentations from submissions on Viewpoints and use cases of potential E2ET&S open architecture and elements
12:30pm	Pick up box lunch en route to breakouts
1:00pm	Breakout working session by focus area to develop proposal for end to end trust and security framework, research challenges, next steps • By use case — e.g., Healthcare, smart grid, connected vehicles – and/or technology elements
3:00pm	Break
3:30pm	Readout from breakouts
4:30pm	Brainstorming Next Steps & Actions
5:15pm	Closing Remarks
5:30pm	End of day