IoT - Submissions

1. **Global Policy Principles for IoT Security**
   Comments: "In recent years, stakeholders in the Internet of Things (IoT) ecosystem have been coalescing around technical guidance to improve device security. For example, NISTIR 8259/8259A, draft ISO/IEC 27402, and CTA-2088 – which maps directly to the CSDE C2 Consensus, a multi-stakeholder effort that received contributions from more than 20 major organizations. An important next step is to ensure a policy environment where the technical guidance is best effectuated. As policymakers in different countries contemplate regulatory and policy approaches to IoT security – e.g., legislation, certification, labeling, procurement and "baseline"/security controls requirements – now is a critical time for the global community to have a conversation around shared policy principles. Notably, later this year, CSDE will publish principles developed by the technology and policy community to facilitate dialogue with policymakers across the world."
2. **Standards: why they are the backbone of IoT and how they are under threat**
   Comments: "Technical standards provide a common basis for wireless and digital technologies, like WiFi and 5G, to interoperate. Ensuring that the patented technology considered essential to these standards (or Standard Essential Patents, SEPs) is available on fair, reasonable, and non-discriminatory (FRAND) terms is critical for the adoption of standards and the promotion of competition, innovation, product compatibility, and consumer choice. But for all the benefits of standards, the system is vulnerable to abuse as a growing number of SEPs are held by patent trolls, or non-practicing entities, that leverage them to extract payments from creators. As demand for digital devices surges, these bad actors are holding consumers, businesses and the economy hostage. This panel will shed light on how consumers, innovation, and the economy are being held hostage by these bad actors, and what the IGF-USA community can do to learn about the issue and make their voice heard. Speakers: ACT for Save our Standards Coalition, Standards body rep (such as IEEE), SOS member (transportation), Apple"
3. **Supply Chain Management, IoT, AI and Security**
   Comments: Supply Chain security is a global challenge that needs both technology and strong public policy to ensure a safe, transparent, and accountable process to ensure secure technology is in place to protect every level of the user.
4. **Confidence measure to create trust**
   Comments: case study to include industry guidelines, standards and NIST baseline
5. **EU-US Trade & Technology Council: A Roadmap for Cooperation on Digital Security**
   Comments: In December, the EU proposed the establishment of an EU-US Trade & Technology Council (TTC). This panel would bring together cybersecurity experts from Europe and the US to discuss where the TTC should focus its efforts to have the greatest positive impact on digital security.