Cybersecurity - Submissions

1. **Supply Chain Security. In light of recent developments, e.g., SolarWinds, proposing this topic as a panel on supply chain security.**
   Comments: There has been extensive recent work conducted on supply chain security. This includes the work of the DHS ICT Supply Chain Task Force and NIST's Key Practices in Cyber Supply Chain Risk Management and DOD's Cybersecurity Maturity Model Certification (CMMC). In light of the SolarWinds incident, these issues, including software assurance are taking on even greater importance. This is proposed as a panel discussion of these issues.
2. **Critical Infrastructure Security**
   Comments: "The Oldsmar water treatment was shocking, but not a surprise for anyone working in critical infrastructure security. Experts had warned and even demonstrated the insecurity of the nation's critical infrastructure for years, but is now finally the time for action. If so, what can be done at a federal level to support overwhelmed state and local governments protect water treatment facilities, power plants and other industrial control systems? Suggested speakers: Bryson Bort, R Street Institute; Cynthia L. Quarterman, Atlantic Council; Brandon Wales, Acting Director, Cybersecurity & Infrastructure Security Agency"
3. **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.
4. **Should the US expand the definition of Critical Infrastructure and what new rules or oversight should that entail.**
5. **Confidence measure to create trust**
   Comments: case study to include industry guidelines, standards and NIST baseline
6. **Cyber diplomacy and US/global Internet infrastructure development/ regulation**
7. **Best Practices in Internet Standards**
   Comments: "Fostering a more secure Internet is a priority for all stakeholders from across the ecosystem. From business and government, to civil society and technical community, confronting security issues is of the utmost importance. Many technical experts are working with policymakers to develop a set of best practices that promote cooperation amongst Internet stakeholders to promote security well into the future. There are many examples of how this work is being done, one such example is the Knowledge-sharing and Instantiating Norms for DNS and Naming Security (KINDNS). KINDNS develops a simple but effective framework for a more secure DNS operation to which operators can voluntarily and easily commit. Other examples include the Mutually Agreed Norms for Routing Security (MANRS) program run by the Internet Society, and the Domain Abuse Activity Reporting (DAAR) program run by ICANN. We would propose a panel of experts from leading organizations to discuss how stakeholders from across the ecosystem are working together to develop best practices and confront the Internet's most pressing security issues. "
8. **Cyber Denial of Service Is Cyber Attack**

Cybersecurity - Submissions

9. **Combatting Ransomware**
   Comments: Ransomware attacks are on the rise, growing 715% in 2020, according to Bitdefender. These attacks are detrimental for any business or organization, especially during the pandemic, but they can also threaten lives with attacks on hospitals and have become known as "the new snow day" for schools around the country. A collaborative approach is needed to stop this rise of this destructive cybercrime.
10. **Trustworthy Tech - What is being done and what more can be done?**
11. **How far behind in security, resilience and trust requirements is the US v other nations**
    Comments: Compare US to UK, EU and AU policies in in sec and trust and cost/benefit and need.