The Dynamic Coalition on Internet of Things
2020 Year-end report
2021 plan of engagement

Our focus in 2020 was on monitoring the development and passage of legislation on standards and guidelines for Internet of Things (IoT) regulations. We also continued the dialog with the industry partners for both the network operators who manage the connections and manufacturers of IoT consumer goods.

U.S.

The tail end of 2020 brought the enactment of the "Internet of Things Cybersecurity Improvement Act of 2020" promising a new scrutiny of security for the Internet of Things ("IoT") by the U.S Federal Government procurement process. While the focus is on IoT devices purchased by the federal government, it is expected to have a significant impact for IoT manufacturers across the economy. It also likely will have important implications for enterprise cybersecurity through its vulnerability disclosure provisions. Many U.S. regulatory agencies have imposed new cybersecurity requirements on critical infrastructure operators that includes all operational technologies including IoT.

- *Standards and Guidelines for IoT Device Management and Security*
- *Vulnerability Management and Disclosure*
- *Enforcement and Waiver applications on best practice models*
- Manufacture IoT devices
- *Security Standards for IoT Across the Economy*
- *Increased Scrutiny on Vulnerability Disclosure Practices*
    - Device configuration
    - Data protection
    - Logical access to interfaces
    - Software update
    - Cybersecurity state awareness
    - New Publications on IoT from NIST

EU

The European Commission launched a sector inquiry into the Internet of Things (IoT) here for consumer-based products and services in the EU in the fall of 2020. The European Commission is expected to publish its final report in Summer 2022. The inquiry will focus on "*consumer-related products and services that are connected to a network and can be controlled at a distance, for example via a voice assistant or mobile device, including smart home appliances and wearable devices*".

Key area of interest for the EU

- Use of data/Data Access

- Sector partnerships, EU will request contractual information when they are not satisfied with the interoperability capabilities

Industry Partners

The Council to Secure the Digital Economy (CSDE) published it's "Convene the Conveners" consensus document in September 2019 to highlight the importance of both the societal and economic benefits of IoT. Since this document was published the technological evolution has been fueled by enhanced broadband connectivity and more connected devices at a global scale with the shift away from the daily office environment towards stay-at-home work, education, and entertainment. This shift also heighted the awareness of security threats brought into more places with the additional IoT equipment deployed across both make-shift offices and home environments.

Much of the Information Communications and Technology (ICT) sector partners recognize the importance of global industry driven standards and best practices to help solve the security challenges and bring a resilience to the IoT device ecosystem. The C2 effort brought together a range of technical experts to be one of the most collaborative efforts for harmonization of technical industry security guidelines for IoT.

C2 has been cited by the National Institute of Standards and Technology (NIST), the Consumer Technology Association (CTA) with ISO/IEC joint technical language under development. These efforts have brought harmonization around technology and design neutrality as part of a consensus based international standard creation. This approach helps ensure a more future proof set of guidelines that can be enables at a global scale.

C2 is working with the DC IoT to ensure the education and leverage of the public-private partnerships and multi-stakeholder efforts as part of the adoption and deployment of best practices and standards for the deployment of more secure IoT devices at a global scale.

These guidelines are being discussed and adopted by multiple cybersecurity programs, certification programs, regulatory bodies, as well as local and country wide legislatures.

The DC IoT will continue to our engagement in 2021 within discussion forum such as EuroDIG, the local and country IGF platforms and the IGF towards the end of 2021 with a joint Dynamic Coalition on Core Internet Values and Internet of Things collaborative session.