# IEEE Conference on Communications and Network Security

## June 10 - 12, 2019//Washington, DC


**Call for Posters**

## Important Dates:

**Paper Submission Deadline:** 5 March, 2019
**Notification of Acceptance:** 26 March, 2019
**Final Poster Submission:** 2 April, 2019

## Poster Chairs:

**N. Kiyavash,** Georgian Institute of Technology, USA
**K. SubbaLakshmi,** Stevens Institute of Technology, USA

The IEEE Conference on Communications and Network Security (CNS) is a premier forum for cyber security researchers, practitioners, policy makers, and users to exchange ideas, techniques and tools, raise awareness, and share experiences related to all practical and theoretical aspects of communications and network security.
IEEE CNS 2019 welcomes poster submissions to be presented during the conference. A poster submission should be a 2-page IEEE conference style, which summarizes the key merits of proposed ideas, presents initial results, and identifies challenges to develop a complete solution. Please include the words "IEEE CNS 19 Poster" under the title. Poster submissions will be evaluated by the Posters Session Committee based on the novelty and the potential to stimulate discussions and promote collaborations. Posters should be submitted via EDAS at http://bit.ly/cns2019posters. Please follow the same template for regular conference papers available on http://www.ieee-cns.org. Sample topics of interest include, but are not limited to:

- Anonymity and privacy technologies
- Censorship countermeasures and privacy
- Combating cyber-crime (anti-spam, anti-phishing, anti-fraud techniques, etc.)
- Computer and network forensics
- Cyber deterrence strategies
- Game-theoretic security technologies
- Implementation and evaluation of networked security systems
- Information-theoretic security
- Intrusion detection, prevention, and response
- Key management, public key infrastructures, certification, revocation, and authentication
- Malware detection and mitigation
- Security metrics and models
- Physical-layer and cross-layer security technologies
- Security and privacy for big data
- Security and privacy for data and network outsourcing services
- Security and privacy for mobile and wearable devices
- Security and privacy in cellular networks
- Security and privacy in cloud and edge computing
- Internet Security: protocols, standards, measurements
- Security and privacy in crowdsourcing
- Security and privacy in cyber-physical systems
- Security and privacy in emerging wireless technologies and applications (dynamic spectrum sharing, cognitive radio networks, millimeter wave communications, MIMO systems, smart/connected vehicles, UAS, etc.)
- Security and privacy in peer-to-peer and overlay networks
- Security and privacy in WiFi, ad hoc, mesh, sensor, vehicular, body-area, disruption/delay tolerant, and social networks.
- Security and privacy in smart cities, smart and connected health, IoT, and RFID systems
- Security for critical infrastructures (smart grids, transportation systems, etc.)
- Security for future Internet architectures and designs
- Security for software-defined and data center networks
- Security in machine learning
- Social, economic, and policy issues of trust, security, and privacy
- Traffic analysis
- Usable security and privacy
- Web, e-commerce, m-commerce, and e-mail security