The Internet Initiative of the IEEE appreciates the opportunity to make a contribution to 2018 IGF Best Practice Forum (BPF) on Cybersecurity focusing on the development of culture, norms and values in cybersecurity. We commend the work of the BPF and its open call for contributions to gain perspectives from all interested stakeholders on existing norms development efforts, how these norms are being implemented and whether they are successful. With this, we respectfully make the following contribution to address the question "**what are the typical values and norms that are important to you or your constituents?**"

As an organization that is committed to developing trust in technologies through transparency, technical community building, partnership across regions and nations, as service to humanity, IEEE believes that measures that reduce the security of information or that facilitates the misuse of secure information systems will inevitably damage trust, which in turn will impede the ability of the technologies to achieve much broader beneficial societal impacts.

IEEE supports the use of unfettered strong encryption to protect confidentiality and integrity of data and communications and opposes efforts by governments to restrict the use of strong encryption and/or to mandate exceptional access mechanisms such as "backdoors" or "key escrow schemes" in order to facilitate government access to encrypted data. Mandating the intentional creation of backdoors or escrow schemes — no matter how well intentioned — does not serve those interests well and will lead to the creation of vulnerabilities that would result in unforeseen effects as well as some predictable negative consequences.

- Strong encryption is essential for the protection of individuals, businesses and governments from malicious cyber activities. Encryption protects confidentiality and integrity of data and communications. Almost all of internet commerce relies on encryption to protect data.
- Exceptional access mechanisms would create risks by allowing malicious actors to exploit weakened systems or embedded vulnerabilities for nefarious purposes. Knowing that exceptional access mechanisms exist would allow malicious actors to focus on finding and exploiting them. Centralized key escrow schemes would create the risk that an adversary would have an opportunity to compromise security of all participants, including those who were not specifically targeted. As a result, the risk of successful cyber-theft, cyber-espionage, cyberattack, and cyberterrorism could increase. The consequences of malicious cyber activities to individuals and society might take many forms — including direct financial losses; identity theft; intellectual property theft and theft of sensitive business information; damage to critical infrastructure; damage to national security; reputational damage; opportunity costs such as lost productivity; and even possibly loss of life when computer systems that support essential functions are disabled. Additionally, by increasing the risk of malicious alterations to data, extraordinary access mechanisms could reduce trust in authenticity of data and might lead to decision-making errors and miscalculations.
- Efforts to constrain strong encryption or introduce key escrow schemes into consumer products can have long-term negative effects on the privacy, security and civil liberties of the citizens so regulated. Encryption is used worldwide, and not all countries and institutions would honor the

policy-based protections that exceptional access mechanisms would require. A purpose that one country might consider lawful and in its national interest could be considered by other countries to be illegal or in conflict with their standards and interests. Thus, issues of jurisdiction may be the greatest impediment to exceptional access mechanisms.

- Law enforcement agencies have a range of other investigative tools to ensure access to systems and data, when warranted. Techniques include legal mechanisms for accessing data stored in plaintext on corporate servers, targeted exploits on individual machines, forensic analysis of suspected computers, and compelling suspects to reveal keys or passwords.
- Exceptional access mechanisms could hinder the ability of regulated companies to innovate and compete in the global market. Required exceptional access mechanisms could open an opportunity for non-regulated market participants to create products and services that may appear to customers in the global market to be more trustworthy than warranted.

This contribution is based on the IEEE Public Policy Position Statement in Support of Strong Encryption that can be found at: http://globalpolicy.ieee.org/wp-content/uploads/2018/06/IEEE18006.pdf