Introduction

Given the increasing need for infrastructure provided by ICT to serve as one of the CENB's founding principles, it should provide a suitable level of security for this infrastructure and services provided on it.

It is the cornerstone of creating and enhancing trust and development assistance to the ICT area. Sustainable development of all levels (organizational, national, and international) is directly related to the protection of all aspects of this infrastructure, including its security dimension.

Cyber security has an enormous impact on increasing the trust and confidence in raising the motivation for SDG. As an example of a comprehensive study, this proposal is the result of achievements in the field of development (maturity) of security And Challenges in the Mobile Communications Company of Iran (MCCI), which is the biggest mobile ICT infrastructure in Iran. Finally, there are suggestions for removing barriers to improving security that are effective in raising the level of trust and sustainable development

Obstacles:

1- Use of information collected for a particular purpose, being repurposed for other, inappropriate purposes. For instance, theft of information from smart meters, smart grids and Internet of Things devices for competitive reasons, or the de-anonymization of improperly anonymized citizen data

   Many information systems, especially in Telco, do not implement the stated security guidelines. Moreover, communicated data related to security monitoring like logs should be not only in a unified format but also in a common language so that similar events in different systems produce similar logs. Similarly important is the identity issue. The mechanisms in place are severely deficient in reliably identifying the genuine source device and user of an event. Thus, the real perpetrators of security breaches cannot be tracked and punished. These three problems constitute the main technical challenges in the way of effectual realization of security monitoring and enforcement.

   From a management viewpoint, it is crucial that all levels of ISP's and Internet coordination and administration bodies lay down protocols to organize coordinated reconnaissance and response operations of malicious activity over the Internet.

   For those issued to be addressed we propose stakeholders from governmental, technical, and international communities to be invited to the forum.

2- Due to unilateral sanctions, barriers and challenges are as follows:
   a. Unavailability of conventional and conventional security equipment
   b. Failure to receive support from equipment manufacturers(Updates and providing information to fix equipment problems)
   c. Failure to attend various conferences and events in the field of security in order to raise the knowledge as well as presenting accumulated knowledge in the collection (for example, the annual FIRST and GSMA conferences)

d. Unavailability of membership in relevant security groups (for example, membership in FIRST) To contribute effectively and continuously to raising security levels at various organizational, national and international levels
e. Limitation on the use of knowledge and experience of foreign companies in the field of security and on use of articles and documentation of hi-tech security companies
f. Limitation on the use of new and safe protocols (the risks of using algorithms such as A5-1)
g. Limitation on the use of licensed products such as operating systems, Database, . …

3- Unauthorized access to devices that take an increasing role in people's daily lives

Based on poor security status in USSD as one of the solutions used in Mobile payment services and important bank transactions, security attacks, such as unauthorized access to sensitive information on USSD subscribers threaten.

There are several major achievements in securing USSD transactions provided by MCI security department. Important one is the solution is the first ever made in the country and in a service provider as well with no similar foreign rival. In order to be the pioneer, this security native mechanism designed in an independence of the solution to cellphone or operating systems technologies with compliance to PCIDSS standard. With the mentioned achievements and many other reasons, we can say there would be a huge impact in the security of banking transaction by using this solution for users.

4- What is for you the most critical cybersecurity issue that needs solving and would benefit most from a multi-stakeholder approach within this BPF?

The following issues are the most important security challenges in developing Mobile Broad Band (MBB) network:

Lack of public and available professional forums to addressing security threats and vulnerabilities in the Telecom core network.
Low awareness of system administrators and managers in securing next generation networks.

One of the biggest security challenges that threatens the future of cyber security is the expansion of the Internet of Things. With the spread of Internet usage in personal and home appliances, there will be new threats due to the lack of security awareness for subscribers and lack of IOT standards (many works in this field is not standardized yet)

5- MCCI also has a good experience on customization of CERT & SOC which can be delivered to BCF

Suggestion:

Given the impact of international security on all the elements involved, raising the security of each element can help to increase international security at a macro level.

Hence, it would be desirable to deal with issues that would impede ICT security in any organization or country, Including listed in the barriers section, in the form of an international partnership, efforts are being made to address them. As noted earlier, considering the ICT platform used by the whole of the world and connections and communications worldwide, undoubtedly, the security of an organization or a country will have a direct impact on international security. By providing, the possibility of constructive exchanges and interactions in this area and addressing the challenges posed by the sanctions, without current constraints, effective action will be taken in line with the main goals of the **IGF**.