International Telecommunication Union International Telecommunication Union

ITU Regional Development Forum for Europe (RDF-EUR)

Information and Communication Technologies for Attaining Sustainable Development Goals

Monday 6 May 2019 | Rome, Italy

https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2019/RDF/Regional-Development-Forum.aspx

CONTRIBUTION BY COMMUNICATIONS REGULATORY AGENCY/ BOSNIA AND HERZEGOVINA

TITLE: Statement of the situation and proposal of activities to enhance trust and confidence in the use of information and communication technologies

CONTACT: Amela Odobasic (ITU DFP), aodobasic@rak.ba, +38761134394

Europe Regional Initiative: EUR4: Enhancing trust and confidence in the use of information and communication technologies

Year(s) of implementation: 2019/2020

Background: **Bosnia and Herzegovina** is in the process of establishing the network of CIRTs in cooperation with other relevant institutions and with the support by ITU-D. ITU-D conducted a Readiness Assessment to Establish a CIRT Network in Bosnia and Herzegovina (BiH) and the final report was submitted in August 2018. However its implementation by BiH state institutions is still pending because strategic decisions are yet to adopted by the Council of Ministers based on the consensus of all relevant institutions in Bosnia and Herzegovina. Communications Regulatory Agency (CRA), Ministry of Security of BiH and Ministry of Transport and Communications of BiH recognized the need to commence the procedure of the implementation of CIRT centers on a national level concerning the cybersecurity threats for the government institutions and public sector.

Proposal: Following the General Elections held in 2018, Bosnia and Herzegovina still waits for the Government to be formed. However, it envisages that in 2019/2020, all preconditions will be met to have the network of CIRT centers in place in full cooperation with the relevant institutions in line with their respective competencies. In achieving the set goals, Bosnia and Herzegovina relies on both ITU as well as on the delegation of European Commission in Bosnia and Herzegovina for further expertise and support, to overcome the challenges and ensure the implementation of Network and Information Security Directive (NIS).

It is believed that strengthening the coordination between the BiH institutions, adopting the Strategy on cybersecurity as well as ensuring the government's unified position on the CIRT network in BiH, are key in overcoming the existing challenges on a national level.

Besides, prior to and in the process of the establishment of the CERT network in Bosnia and Herzegovina, it is necessary to:

- Provide regional/national platforms, tools and opportunities for building human capacities (awareness and expert training - ICT professionals into the expert level for cybersecurity in cooperation with universities, significant ICT companies and with the support by ITU-D);
- Provide training to improve the skill-sets and competency of the personnel who will be manning the CIRT Network in BiH in areas of cybersecurity as well as to build their confidence in carrying out their duties;
- Improve the overall readiness, availability, and reliability of ICT infrastructure and services to the different institutions of Bosnia and Herzegovina;
- Develop applicable policies and regulations for the ICT systems of the institutions of Bosnia and Herzegovina;
- Provide international support/guidance in overcoming the lack of education /knowledge on the cybersecurity and the lack of awareness as challenges in enhancing trust and confidence in the use of information and communication technologies, and, in particular, ensure necessary capacity building for persons responsible for managing the CERT network;

Although a developing country like Bosnia and Herzegovina faces several fundamental issues such as the construction of basic infrastructure, it is important that the Government CIRT is established before a critical attack occurs. The establishment of a Government CIRT in Bosnia and Herzegovina should be seen as a long-term investment and as a building block onto which other cybersecurity projects can be developed.