

## REPUBLIC OF SERBIA

### **Resolution 68/243 “Developments in the field of information and telecommunications in the context of international security”**

Taking into account the great importance given to information security on the global and national level, the Republic of Serbia undertakes a number of activities in order to provide efficient national policies and effective security mechanisms. In the Strategy of Development of Information Society in Republic of Serbia until 2020, adopted by the Government of the Republic of Serbia in 2010, information security is declared to be one of six priority areas. Serbia does not have national strategy singularly dedicated to information security, but this topic is carried by a number of other documents. In October 2013, a special workgroup was formed with tasked to draft The Law on Information Security. The Law is harmonized with the relevant international and EU legal framework and it determines the following: information security institutional framework; measures needed to provide enhanced security of ICT systems in the Republic of Serbia, including ICT systems of public bodies and enterprises; norms for prevention coordination of security risks in ICT systems; establishment of the national Computer Emergency Response Team (CERT); specific security measures and preconditions to be applied in information systems of state bodies; security of classified data in ICT systems; crypto-security and protection from compromising electromagnetic emanations.

The ICT Department of the Administration for joint services of the republic bodies performs the activities in protecting of information security, data protection and implementation of prescribed security standards for information systems of state bodies. In the Administration's annual report, they state that within their mandate of protection of state ICT systems, the Department provides protection from cyber-attacks on a daily basis, as the network is attacked every day.

The Academic network of the Republic of Serbia (AMRES) performs the CSIRT activities for the educational and scientific-research institutions in the Republic of Serbia. In the AMRES 2013 Annual Report, it is declared that there is an increasing number of incidents compared to the year 2012. The Report identifies old equipment is one of the reasons for the increasing number of attacks.

Only well established national information security culture embraced at the every level of the society can be locally effective to strengthen the security of national information and telecommunications systems. Similar, only such well established national information security systems can be a part of the application of the international information security concepts to strengthen the security of global information and telecommunications systems.

The Office of the National Security Council and Classified Information Protection (hereinafter: NSC Office) is the Serbian Government's service responsible for coordination of implementation of the national and the EU security policies at the national level (*National Security Authority - NSA*). A specific segment of its activities is reflected in the passage and coordination of implementation of Information Assurance (IA) measures in government bodies and other institutions for the purpose of CI protection. In this context, the Decree on special measures for the protection of classified information in information-telecommunication systems was passed in 2011 (Official Gazette RS, No. 53/2011). At the international level, since 2011 the NSC Office has been an active participant in the Forum of the South East European National Security Authorities' directors (SEENSA). One of the Forum's primary aims is to enhance IA and classified information protection in the regional countries in line with international standards. The NSC Office acts as a chief coordinator for developing a regional cyber defense concept within SEENSA framework.

The NSC Office has prepared and sent other TWG members a number of related proposals for their examination, harmonization and approval. Such proposals are structured by means of the following working documents: 1.- Cyber Defense Program Objectives, and 2. - SEENSA Cyber Defense Questionnaire;

Ministry of Defense of the Republic of Serbia is participating in the implementation of the UN Resolution 68/243. Departments within the Ministry of Defense are active in the workgroup which is tasked to draft The Law on Information Security.

Also, the Ministry of Defense is in the process of forming different departments that will operate in the area of Information Security and cyber defense.