Summary of the audit report Efficiency of ensuring cybersecurity in the Republic of Slovenia

The Court of Audit implemented the audit of the efficiency of **the Government of the Republic of Slovenia**, **the Government Office for the Protection of Classified Information** and **the Ministry of Public Administration** in ensuring cybersecurity in the Republic of Slovenia in the period from 1 January 2016 to 30 September 2019. According to the opinion of the Court of Audit, the Government, the Office for the Protection of Classified Information and the Ministry were inefficient in the period covered by the audit.

In February 2016, the Government adopted Cybersecurity Strategy – setting up the system of providing high level of cybersecurity, and in April 2018, upon the proposal of the Government the Information Security Act was adopted which transposed into the Slovenian law the Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. The Government should in one year adopt the Information Security Strategy but it failed to do so even by the end of the period covered by the audit. The list of essential services and the methodology for determining providers of essential services were defined with more than a 7-month delay by the Government. Since it failed to timely determine the providers of essential services, the Government received a letter of formal notice from the European Commission. The Government did not determine state bodies that manage information systems and parts of the network respectively implement information services necessary for undisturbed operations of the state or for providing national security. Despite the fact that the Government adopted Cybersecurity Strategy at the beginning of 2016 and authorised the Office for the Protection of Classified Information for the implementation of the tasks related to cybersecurity, it failed to adopt an action plan or other operational document for the implementation of measures related to ensuring cybersecurity. Furthermore, the Government failed to provide resources for the implementation of Cybersecurity Strategy. In 2019, it provided conditions for setting up both bodies foreseen in the Information Security Act, but it did not analyse personnel and technological needs and it did not in due time provide sufficient funds for personnel and technological strengthening of the cybersecurity field. Also in 2019, it set up Office for the Protection of Classified Information, namely a few months before the deadline defined by the Information Security Act. The Government failed to introduce new programmes of rising the awareness in the field of cybersecurity and it failed to introduce contents from the concerned field in the educational and training system.

The Office for the Protection of Classified Information defined the field of cybersecurity within the framework of its organisation in line with decree of the Government, but it implemented the activities only in the limited scope due to personnel and financial shortfall. It actively participated in international drills from the field of cybersecurity and within international working bodies and associations, while a national exercise of cybersecurity was not carried out due to lack of resources. The Office for the Protection of Classified Information began to receive information on incidents in the field of cybersecurity from national centre SI-CERT and the Ministry from January 2019 and it regularly informed the National Safety Council on situation concerning cybersecurity.

The Ministry adopted the Rules on security documentation and security measures of operators of essential services with a delay of several months, while it adopted the Rules on security documentation and security measures of state administration authorities with a 12.5-month delay. The Ministry failed to develop a proposal for information security strategy which was foreseen in Information Security Act respectively it did not assess whether the existing information security strategy should be updated or amended due to new legislation. Therefore, it undertook a cyber risks assessment, but it failed to analyse the situation in the field of cybersecurity which would be the basis for the assessment of needs and for providing appropriate sources, furthermore the assessment did not include proposals of individual tasks to improve cybersecurity. The Ministry did not provide for the implementation of awareness-rising programmes in the field of cybersecurity, it thus provided resources for the operations of the SI-CERT and developed internal courses for information security. The Ministry set up the Computer Security Incident Response Team in a timely manner, it participated in international exercises in the field of cybersecurity, and also in international working bodies and associations. Nevertheless, it failed to thoroughly monitor how conditions were ensured and how tasks were implemented in the field of cybersecurity in line with the Information Security Act, since providers of essential services were not determined. The Ministry did not adjust measures in the field of cybersecurity which would be based on the analysis of monitoring the ensuring of cybersecurity.

The Court of Audit demanded from the Government and the Ministry to submit **response reports** in which they must present corrective measures, and it also proposed **recommendations** to improve the situation.

Ljubljana, 3 March 2021