Audit Report on audit No

19/26

Building the National Cyber security of the Czech Republic

The audit was included in the audit plan of the Supreme Audit Office (hereinafter the "SAO") for 2019 under number 19/26. The audit was managed and the audit conclusion was drawn-up by a member of the SAO, Ing. Roman Procházka.

The aim of the audit was to verify whether the activities of the main entities involved in ensuring the cyber security of the Czech Republic and the degree of efficiency of their mutual cooperation actually lead to its increase in terms of objectives and activities defined by the *National Cyber Security Strategy of the Czech Republic for the Period from 2015 to2020 and the Action Plan for the 2015-2020 Strategy*.

Audited entities:

National Cyber and Information Security Agency, Brno (hereinafter also "NCISA"),
Ministry of the Interior ("MoI").

The audit of these audited entities was performed between October 2019 and June 2020.

Audited period: 2015 to 2020.

Note: The legal regulations referred to in this Audit Conclusion are applied as effective in the audited period.

The Board of the SAO at its XIV meeting held on 14 September 2020

issued Resolution No 8/XIV/2020 approving

the ***Audit Conclusion*** as follows:

National Cyber Security of the Czech Republic in figures

Czech Republic

348 information systems[1]

111 critical information infrastructure (CII) systems
179 major information systems (MIS)
58 basic services information systems (BSIS)

CZK 2 787 million[2]

Estimated total funds spent by the ministries and the Office of the Government of the Czech Republic to ensure cyber security over the years 2015 to 2019

National Cyber and Information Security Agency

916

The number of cyber incidents reported to the governmental CERT from 2017 to mid-2020, of which 31% were incidents encountered in the first half of 2020.

CZK 884 million

Expenditures in the NCISA chapter since its establishment until the end of 2019

CZK 112 million

Funds of Call No 10, which NCISA used within 2 projects focused on cyber security

Ministry of the Interior

19 information systems[3]

12 CIIs
7 MISs

CZK 750 million[2]

Estimated funds spent by MoI to ensure cyber security over the years 2015 to 2019

CZK 0

MoI did not draw any funds under Call No 10.

[1] **CII** - a system in which a defect in functioning would have a serious impact on national security, provision of basic living needs of the population, human health or the national economy, **MIS** - a system in which a defect in information security may compromise or significantly jeopardize the exercise of power of public authorities, **BSIS** - a system whose operation determines the provision of basic services and the disruption of which could have a significant impact on the security of social or economic activities in any of the following sectors: energy, transport, banking, financial market infrastructure, healthcare, water management, digital infrastructure, chemical industry.

[2] This is an estimate of funds as obtained from NCISA through the questionnaire surveys conducted over the years 2018 and 2019 at selected organisational units of the state.

[3] The data relates exclusively to the organisational unit of the state, the Ministry of the Interior. Nevertheless, cyber security is being addressed at the Ministry of the Interior at the level of the department. As regards the Ministry of the Interior, there are a total of 30 information systems (19 CIIs and 11 MISs). For detailed information, see Part II of this Audit Conclusion.

I. SUMMARY AND EVALUATION

The audited entities were: NCISA, which oversees the cyber and information security of the state, and the Ministry of the Interior, which among other functions as the central body for state administration of information systems, electronic identification and trust services. NCISA was established on 1 August 2017 to take over the agenda of national cyber security (hereinafter also "CS") from the National Security Authority (NSA). Total expenses incurred by NCISA in connection with the performance of its activities over the years 2017 - 2019 amounted to approximately CZK 884 million. The audit examined the activities of NCISA and MoI in the areas of setting up and subsequent ensuring of cyber security of the Czech Republic (hereinafter also abbreviated to "CR") and meeting the objectives and tasks of *the National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020* and the *Action Plan for the National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020* (hereinafter also abbreviated to "AP CNCS"). According to the results of the questionnaire surveys conducted by NCISA in 2018 and 2019, ministries and the Office of the Government of the Czech Republic spent an estimated CZK 2.8 billion on ensuring the cyber security of the state between the years 2015 and 2019.

The SAO verified by audit that the activities of the main entities involved in the provision of cyber security of CR and the degree of effectiveness of their mutual cooperation has led to the increase of cyber security. The increased cyber security of the state and the degree of effectiveness of cooperation between NCISA and the MoI were evaluated by the SAO on the basis of an actual fulfilment of 57 selected tasks set out in AP CNCS[4]. NCISA and MoI managed to fulfil most of these tasks in the audited period from 2015 to 2020. Of the 57 tasks examined, the SAO found shortcomings in only eight.

The Ministry of the Interior (MoI) is the central state administration body, inter alia, in the area of information systems (hereinafter also abbreviated to "IS") of public administration. The MoI[5] is the most important department of state administration in terms of the number of managed systems of critical information infrastructure and important information systems. The MoI stated that in order to meet the requirements arising from Act No 181/2014 Coll., on Cyber Security and on Amendments to Related Acts (Act on Cyber Security, hereinafter also “AoCS”), the Ministry of the Interior lacked by 2020[6] , according to the results of a questionnaire survey conducted by NCISA, approximately CZK 309 million. Despite the stated lack of funds in the state budget, the Ministry of the Interior failed to use Call No 10 – *Cyber Security* (hereinafter also referred to as “Call No 10”) and did not draw funds from the EU funds allocated in the 2014+ programming period to increase cyber security. The Ministry of the Interior participated in the specification of Call No 10 in co-operation with the Ministry of Regional Development and other entities. Concurrently, the SAO found that the MoI failed to annually implement part of the measures proposed in the

[4] SAO examined 57 of the total of 141 tasks set out in AP CNCS. The SAO selected for the audit tasks primarily from AP CNCS, the fulfilment of which required the cooperation between the Ministry of the Interior and NCISA or where NCISA or MoI functioned as the responsible entity. Yet, these were not all tasks under the responsibility of NCISA and MoI.

[5] Cyber security is addressed at the Ministry of the Interior from a departmental point of view through a unified information security management system.

[6] The aim of the NCISA questionnaire survey in 2018 and 2019 was to find out the difference between the level of funds for cyber security and their need in 2020.

individual risk management plans[7], which represents an increased security risk in terms of cyber security.

Authorized applicants[8] could draw funds for the cyber security-related projects within Call No 10, up to the amount of CZK 1.3 billion. Call No 10 was announced by the Ministry of Regional Development on 21 October 2015. The NCISA drew a total of CZK 112 million from Call No 10 for two projects. The largest volume of funds within Call No 10 (approximately CZK 903 million) was channelled to cyber security-related projects in health care facilities, a big part of which does not fall within the entities managing CII, MIS or BSIS as per the applicable criteria. In relation to the ongoing computerisation of health care, the need for investment in cyber security-related information and communication systems in health care facilities through Call No 10 was substantiated.

Nevertheless, cyber attacks at the turn of 2019/2020 directed against health care facilities showed that even if they were not mandatory entities under AoCS, a series of cyber attacks on these facilities would have a significant impact on the functionality of the Czech health care system.

The ability of NCISA and MoI to fulfil the cyber security key activities depended on professional and highly specialised personnel capacities, the provision and maintenance of which remain problematic for the state administration on a long-term basis.

The cooperation between NCISA and MoI was not formally established until the end of the audit, which was to take place through the fulfilment of selected tasks within AP CNCS. Among others, a detailed model and scheme of cooperation in the field of cyber security were to be created. The cooperation thus works mainly at an informal level and on an ad hoc basis, depending on current needs, which the SAO verified on the example of dealing with current cyber attacks. However, in the opinion of the SAO, this situation represents, on a long-term basis, a risk for maintaining the continuity of cooperation and the necessary ability to act in the event of personnel changes in both or one of the audited institutions.

The overall evaluation is based on the following facts:

Fulfilment of tasks within AP CNCS

The NCISA and the MoI managed to successfully fulfil most of the 57 tasks audited by the SAO within AP CNCS. Partial shortcomings were identified by the SAO in eight tasks. Those primarily concerned the setting up of cooperation of the key cyber security actors. The effectiveness of cooperation between the NCISA, the MoI and other entities may be negatively affected in the future by the fact that it has not yet been formally set up and stabilised between these bodies. This was also to take place within the selected AP CNCS tasks audited by the SAO. Yet, the cooperation is based on personal ties and ad hoc problem-tackling where necessary.

Despite the aforementioned, the cooperation between the NCISA and the MoI in dealing with extraordinary cyber events worked quite well. At the turn of 2019-2020, both audited institutions jointly participated in the management of cyber attacks on health care facilities[9].

[7] These are the basic documents of the Ministry of the Interior governing its intentions in the area of cyber security.

[8] I.e. organisational units of the state, subsidised organisation of OUS, state organisations, state enterprises, regions, organisations established or founded by regions, municipalities (except Prague), organisations established or founded by municipalities (except Prague).

[9] Even for entities that were not subject to the obligations arising from the AoCS.

However, the personnel capacities of the NCISA and the MoI are very limited in the event of several concurrent extraordinary events.

Financing the National Cyber Security

Despite the announced expenditure of CZK 2.8 billion for the period between the years 2015 and 2019, the ministries and the Office of the Government of the Czech Republic lacked - according to their estimate[10] - the order of hundreds of millions of Czech crowns for the complete cyber security in accordance with the requirements of Act No 181/2014 Coll., on cyber security and on amendments to related acts (Act on Cyber Security). The estimate calculated by the Ministry of the Interior was CZK 309 million. The MoI is the most important department of state administration in terms of the number of managed CII[11] and MIS systems of critical information infrastructure and major information systems. In total, the MoI managed 19 CIIs and 11 MISs as of 2020. The development of the number of cyber attacks on IS shows a growing trend. In recent years, these attacks against the MoI have increased by at least 220%.

In relation to the financing of cyber security, the SAO detected shortcomings in the system for monitoring funds incurred. During the audited period, the NCISA did not have information on the total amount of funds incurred within individual chapters of the state budget or the entire national budget for cyber security, and in order to determine their amount in 2018 and 2019 it carried out four questionnaire surveys at ministries and the Czech Government Office. In the case of the MoI, the funds spent on cyber security were not systematically and regularly monitored, which represents a restriction for the fulfilment of the set obligation for the chapter administrator to systematically monitor and evaluate the economy, efficiency and effectiveness of spending in this chapter.[12]

The area of human resources is also closely connected to the area of funds. Acquiring and maintaining professional capacity is an ongoing challenge for both institutions. The NCISA has long struggled with the fluctuation of professional employees at the level of 10%. The Ministry of the Interior has also been struggling for long with high fluctuation in the relevant job positions and has arranged for some key security roles externally, despite the fact that it can use the institute of a key service position, as it is covered by Act No 234/2014 Coll., on civil service.

Use of ESIF funds for cyber security

In the audited period, ministries and other entities had the opportunity to draw funds from the European Structural and Investment Funds (hereinafter also abbreviated to “ESIF”) for projects in the cyber security area within the Call *Integrated Regional Operational Programme* (hereinafter also abbreviated to “IROP”) No 10 – *Cyber Security*, up to CZK 1,340 million. After the assessment by the Managing Authority, projects implemented by the state sector accounted for CZK 799.6 million, of which only CZK 121 million[13] was allocated to the projects

[10] This is an estimate of funds as obtained from the NCISA through the questionnaire surveys conducted over the years 2018 and 2019. The SAO has not verified this estimate.

[11] According to the AoCS, these are information and communication systems of critical information infrastructure. For the sake of simplification, the term "critical information infrastructure systems" and the abbreviation "CII" are used in the Audit Report.

[12] Section 39 of Act No 218/2000 Coll., on Budgetary Rules and on Amendments to Certain Related Acts (Budgetary Rules).

[13] Data source: MS2014+ information system; for more see Chapter IV of this Audit Conclusion.

implemented by the central state administration bodies. In addition, NCISA projects accounted for CZK 112 million out of this amount. Despite its position within the state administration, the Ministry of the Interior did not draw funds within Call No 10. The MoI submitted two aid applications in November 2017, i.e. more than 2 years after the announcement of Call No 10. However, due to the excess of applications over the allocation of the call, these applications were rejected by the Managing Authority. The largest volume of funds from the total allocation within Call No 10 (approximately CZK 903 million) went to projects of health care facilities, some of which could submit applications for their projects only after the expansion of the range of supported activities within Call No 10, i.e. 19 months after its announcement.

Based on the facts found by the audit, the SAO recommends the NCISA, within the scope of the entrusted coordination role, to examine the setting of the criteria for the determination of providers of basic services in the healthcare sector and, if necessary, revise them.

II. INFORMATION ON THE AUDITED AREA

The NCISA is the central administrative office for cyber security. It was established on the basis of Act No 205/2017 Coll., amending Act No 181/2014 Coll. on cyber security, amending related acts (Act on Cyber Security); as amended in Act No 104/2017 Coll. and certain other acts. The NCISA was established on 1 August 2017 to take over the agenda of national cyber security from the National Security Authority (NSA). Among other things, the NCISA is to provide prevention, education and methodological support in the area of cyber security and in selected areas of protection of classified information, issue measures and act as a coordinating body in a situation of cyber danger. It also analyses and monitors cyber threats and risks. The NCISA also performs relevant inspection according to AoCS. Total expenses for the activities of the NCISA over the years 2017-2019 amounted to approximately CZK 884 million.

By virtue of Act No 2/1969 Coll. on the Establishment of Ministries and Other Central State Administration Bodies of the Czech Republic, the MoI performs, inter alia, the coordinating function for information and communication technologies. As of 31 January 2020, the MoI managed a total of 12 CIIs, which represented 22% of all CIIs administered by OUS. From the point of view of the Ministry of the Interior, i.e. after the inclusion of other 7 CIIs, this share represented about 35%. As of 31 January 2020, the MoI also managed 7 MISs, or 11 from a departmental point of view, i.e. when MISs administered by the Police of the Czech Republic (hereinafter also abbreviated to "PCR") and the Administration of Basic Registers are included.

Cyber Security

Cyber Security is a specific area of computer technology. Its aim is to ensure the protection of information and property against theft, misuse, corruption or natural disaster, while the protected information must remain accessible to its users. The legal framework of national cyber security and the rights and obligations of public administration entities are defined in the AoCS and its implementing regulations.

Government CERT (GovCERT)

The Government CERT department is also a part of the NCISA. The role of this department is to act as the primary source of security information and assistance for state authorities, organisations and citizens. It is critical in the protection of CII and MIS according to the AoCS and its implementing regulations. It also plays an equally important role in increasing the education in the field of Internet security.

National Cyber Security Strategy for the Period from 2015 to2020 and AP CNCS

The NCISA and the MoI are significantly involved in the development of information and communication technologies (hereinafter also abbreviated to "ICT") in the public administration of the Czech Republic and its security. As regards cyber security, the NSA published the *National Cyber Security Strategy for the Period from 2015 to2020*. The strategy was approved by the Government Resolution No 105 of 16 February 2015. On 25 May 2015, AP CNCS was approved by Government Resolution No 382. The action plan contained a total of 141 tasks divided between individual ministries and other public administration bodies. The aforementioned strategy and AP CNCS go beyond the provisions of the AoCS in some areas.

III. SCOPE OF AUDIT

The aim of the audit was to verify whether the activities of the main entities involved in ensuring the cyber security of the Czech Republic and the degree of efficiency of their mutual cooperation actually lead to its increase in terms of objectives and activities defined by the *National Cyber Security Strategy of the Czech Republic for the Period from 2015 to2020* and *the Action Plan for the 2015-2020 strategy*. In connection with the aforementioned, the SAO also examined the implementation of three projects in the area of cyber security. Two of these projects were implemented by the NCISA and one project was implemented by the MoI.

The NCISA oversees the cyber and information security of the state and the fulfilment of obligations set out in AoCS. The MoI is the central state administration body in the area of public administration information systems, electronic identification and trust services. Concurrently, the MoI or its sector manages 30 IS (19 CIIs, 11 MISs) covered by the AoCS. The increased cyber security of the state and the degree of effectiveness of cooperation between the NCISA and the MoI were evaluated by the SAO on the basis of selected tasks set out in AP CNCS. Of the total 141 tasks set out in AP CNCS, the SAO selected 57 tasks with regard to their responsible entities and co-responsible entities and with the view to examining primarily those tasks that require the cooperation between the NCISA and the MoI.

For the NCISA the audit focused on the activities of this office from the point of view of the body responsible for national cyber security. Total expenses incurred by the NCISA in connection with the performance of its activities over the years 2017-2019 amounted to approximately CZK 884 million. These included activities in the areas of: financing of national cyber security, personnel capacity of the NCISA for the provision of cyber security, cooperation between the NCISA and the MoI in selected activities and NCISA's share in setting out the rules for drawing funds from the European Structural and Investment Funds (ESIF) for cyber security. Furthermore, the SAO focused on the economy and effectiveness of spending funds on the *Cyber Security Incident Detection System* projects *in selected public administration information systems* and the *External Perimeter Protection project*.

As regards the MoI, the audit focused, among other things, on the planning and development of cyber security of IS managed by the ministry, providing for financing of the cyber security development, MoI's personnel capacity in this area, MoI and NCISA cooperation in selected activities and MoI's share in setting out the rules for drawing ESIF funds for cyber security.

Furthermore, the SAO focused on the effectiveness of spending funds on the project of the eGovernment Monitoring Centre (hereinafter also abbreviated to "eGOVMC").

In connection with current events, the SAO also examined the activities of the NCISA and the MoI in managing the cyber attacks on health care facilities and other entities, especially in connection with the utilisation of their personnel capacities.

The audited volume of funds amounted to CZK 828,828,806.

IV. DETAILED FACTS ASCERTAINED BY THE AUDIT

Fulfilment of tasks within AP CNCS

Increasing the cyber security of the state and the degree of effectiveness of cooperation between the NCISA and the MoI was assessed by the SAO mainly on the basis of fulfilment or non-fulfilment of selected tasks within AP CNCS and cooperation of the above-mentioned entities in fulfilling these tasks. Out of the total number of 141 tasks set out in AP CNCS, the SAO examined the non/fulfilment and cooperation within 57 selected tasks. The SAO selected these tasks with regard to their responsible entities and co-responsible entities and with the view to examining primarily those tasks that require the cooperation between the NCISA and the MoI. As part of the fulfilment of the obligation based on the Resolution of the Government of the Czech Republic No 382 as of 25 May 2015, the NCISA defined prerequisites for cooperation with representatives of individual entities that participate in the fulfilment of the AP CNCS tasks. The SAO detected partial shortcomings in 8 tasks, especially in relation to setting up and stabilisation of the cooperation among the key cyber security actors.

Table 1: Examined tasks of AP CNCS with identified shortcomings

Measure ID number in AP CNCS	Text	Responsible entity	Co-responsible entity	Status
A.1.01	In coordination with other entities, establish a scheme and a detailed model of cooperation for ensuring cyber security	NCISA	MoI	The task was not fulfilled on the part of NCISA, the Ministry of the Interior (MoI) did not participate in the task
A.1.02	Carry out an analysis of agendas in the field of cyber security and based on the analysis, define national interests and priorities in this area	NCISA		Task not completed
A.1.03	Carry out technical and non-technical national cyber security exercises	NCISA	MoI	The task was fulfilled on the part of NCISA, partially completed by MoI
A.2.02	Create a communication matrix between the top actors in cyber security (national actors, CII, MIS)	NCISA		Task partially completed

Measure ID number in AP CNCS	Text	Responsible entity	Co-responsible entity	Status
A.4.01	Create an effective model for sharing information on foreign activities between NSA and other relevant entities	NCISA	MoI	The task was fulfilled on the part of NCISA, MoI did not participate in the task
C.5.02	Based on the completion of security mapping for CII and MIS, establish an automated platform for sharing information on cyber security threats and incidents with selected vulnerable entities	NCISA		Task not completed
G.2.03	Jointly plan individual purchases for executive workplaces of OIK and expert workplaces of computer analysis with a guarantee of tied planned funds in planned budgets for the next period	MoI (Police of the Czech Republic)		Task not completed
G.5.01	Extend qualification training courses with basic knowledge and skills related to crime committed in the information technology environment and introduce an electronic or similarly widely deployable system of continuous education	MoI (Police of the Czech Republic)		Task partially completed

Source: prepared by the SAO.

Objective A.1.01 was not fulfilled, as neither NCISA nor MoI submitted any document depicting a scheme and a detailed model of cooperation in ensuring cyber security. The cooperation between the NCISA and the MoI works mainly on an informal level and with regard to current needs.

Objective A.1.02 was not fulfilled because the NCISA did not submit any outputs of the analysis of agendas related to cyber security issues or the definition of national interests and priorities in this area.

The NCISA fulfilled the objective A.1.03, as in the years 2015 to 2019 a number of cyber security exercises of technical and non-technical nature were performed. The Ministry of the Interior, as the co-responsible entity, only partially fulfilled this goal, as it was to participate in these exercises on an ongoing basis, but in fact participated in three exercises only, in 2018 and 2019.

Objective A.2.02 was only partially fulfilled by the NCISA, as it created a database of contacts, but failed to create a communication matrix between cyber security top actors, which was supposed to be created according to the objective set out in the action plan.

Objective A.4.01 was already met by the NSA in 2015 (before the establishment of the NCISA) as it created a model for sharing information on foreign activities and set up a framework for cooperation between the NSA/NCSC and other relevant entities. To this end, a task force has been set up to harmonize international activities at national level. The MoI did not participate in the task as a co-responsible entity.

The NCISA failed to meet objective C.5.02 as it did not, within 4 years after the deadline, establish an automated platform for sharing information on cyber security threats and incidents with selected vulnerable entities, based on the completion of security mapping for CII and MIS.

The Ministry of the Interior (Police of the Czech Republic) did not meet the objective G.2.03, as the planned purchases of HW and SW were not made from tied (guaranteed) planned funds, but from European funds and extraordinary subsidies in the amount of CZK 30 million (a transfer of funds within the MoI chapter). Until the end of the inspection, no funds were approved for the periodic replenishment of material and technical equipment, which may negatively affect sustainability.

The Ministry of the Interior (Police of the Czech Republic) fulfilled task G.5.01 partially, as it failed to introduce an electronic or other similarly widely applicable system of continuous education by the end of the audit. Qualification training courses were extended by the MoI (Police of the Czech Republic) with basic knowledge and skills related to crime committed in the information and communication technology environment.

The cooperation between the NCISA, the MoI and other bodies providing national cyber security has not yet been formally established and stabilised. This was supposed to take place within the performance of some of the aforementioned tasks set out in the AP CNCS, primarily task A.1.01 - *In coordination with other entities, establish a scheme and a detailed model of cooperation for ensuring cyber security*, and cooperation between these entities is based mainly on personal ties and ad hoc agreements.

In connection with the setting of the transmission of evaluation reports on the fulfilment of individual tasks within AP CNCS, the SAO warns that the system set up by the NCISA failed to receive any reports on the fulfilment of AP CNCS from any of the interviewed entities. For example, in 2015, 2016 and 2018, the Ministry of the Interior did not provide the NCISA with all required information on tasks under its responsibility or co-responsibility, and at the same time it did not proceed in accordance with Section 21 of Act No 2/1969 Coll. as it failed to provide coordination in fulfilling AP CNCS Task III/1b imposed by the Resolution of the Government of the Czech Republic No 382 of 25 May 2015.

In addition to fulfilling AP CNCS, the SAO also examined other cyber security areas requiring the cooperation of the NCISA and the MoI. The SAO verified that the NCISA actively cooperated with the Ministry of the Interior in the area of preparation of legal regulations both on the very wording of individual materials and on other related documents. The NCISA as the responsible entity also issued recommendations aimed at individual areas of the AoCS and communicated with the Office of the Chief eGovernment Architect at the Ministry of the Interior (hereinafter also abbreviated to “OCA”) when assessing ICT projects related to cyber security. This communication took place irregularly in the form of official letters, especially when the need arose to consult issues related to cyber security.

From December 2019 to the end of the SAO's audit, a number of significant cyber attacks took place in the Czech Republic, with particular impacts on the operation of hospitals. The first case occurred on 11 December 2019 in Benešov hospital. Another attack took place on 13

March 2020, when the computer network of the Brno University Hospital in Bohunice was attacked. The NCISA and the MoI participated in the solution to these cyber incidents, even where this incident occurred at an entity that did not fall in the category of the so called "mandatory entities" as per AoCS[14]. However, in case of several concurring incidents, there is a risk that the NCISA and the MoI would not have sufficient personnel capacities to cope with them.

Financing the National Cyber Security

The NCISA, i.e. the State, did not have information during the audited period about the total amount of funds spent within individual chapters of the state budget or the entire State on cyber security. In view of the aforementioned absence of information about funds spent and the need to obtain these funds, inter alia, in connection with the new Decree No 82/2018 Coll., on security measures, cyber security incidents, reactive measures, filing requirements in the field of cyber security and data disposal (Decree on Cyber Security), in 2018 and 2019, the NCISA conducted a total of four questionnaire surveys at ministries and the Office of the Government of the Czech Republic[15].

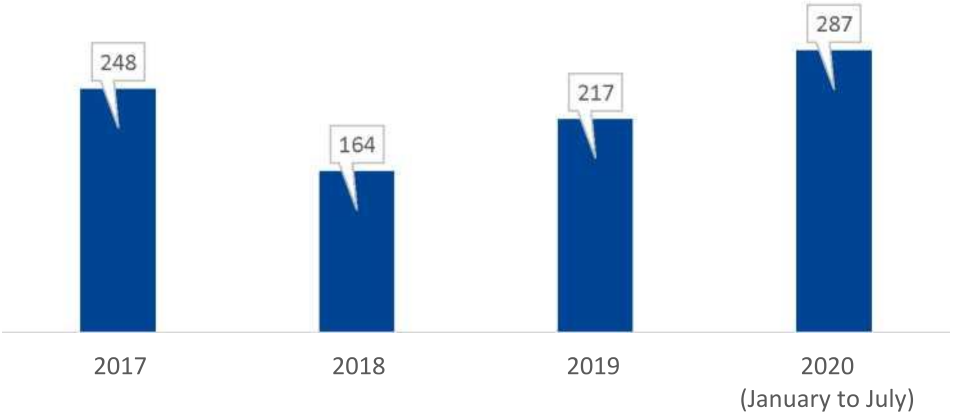
The questionnaire surveys conducted by the NCISA imply that the ministries and the Office of the Government of the Czech Republic spent on ensuring the cyber security of information systems, as per AoCS, an estimated CZK 2.8 billion between the years 2015 and 2019. As regards the Ministry of the Interior, the estimated total funds spent on cyber security in the period 2015-2019 were approximately CZK 750 million (for the chapter administrator only). As of 2020, the respondents of the NCISA's questionnaire surveys quantified the necessary (missing) funds for securing cyber security in accordance with the requirements of the AoCS in their chapters in the order of hundreds of millions of Czech crowns. The estimate calculated by the Ministry of the Interior was CZK 309 million. The SAO examined that the MoI failed to implement in certain parts of cyber security all the measures proposed in the individual risk management plans[16], which represents an increased security risk in terms of cyber security of the MoI. These include measures in the following areas: eGOVMC development, securing certain CIIs and MISs as per AoCS or the development of an information security management system. In the audited period, the Ministry of the Interior faced an increasing number of cyber attacks, as they increased by at least 220% compared to those encountered over the years 2016-2019. For example, in 2019, the Ministry of the Interior registered 397 cyber attacks. Even from the point of view of the whole Czech Republic, the number of cyber attacks has increased in recent years, which is related to the growing number of cyber incidents that were reported to the governmental CERT or to the NCISA. In the first 6 months alone, more incidents were reported to the NCISA than in the whole year 2019, which is illustrated in the following chart.

[14] The NCISA participated in the solution to incidents according to the provisions of Section 20 (l) of Act No 181/2014 Coll., which allows it to participate in the resolution of a cyber incident even for entities that are not listed in the provisions of Section 3 of AoCS as long as it has a serious impact and is subject to NCISA's sufficient capacities. The MoI participated in the solution of the Benešov incident at the request of the NCISA, as it already had experience of a similar type of attack.

[15] Prior to the surveys carried out by the NCISA in 2018 and 2019, the Ministry of the Interior also carried out a similar survey.

[16] These are the basic documents of the Ministry of the Interior governing its intentions in the area of cyber security.

Chart 1: Development of the number of cyber incidents reported to the governmental CERT



Source: Prepared by the SAO on the basis of NCISA data.

The area of human resources is also connected to the area of funds. The fluctuation of NCISA employees - specialists performing professional activities - was at the level of 10%, which in the long run represents a risk of reducing the ability to provide cyber security to the state. In the case of the Ministry of the Interior, the ensuring of implementation of AoCS and for setting up, operating, developing and controlling the system for ensuring cyber security[17], were the responsibility of a Cyber Security department. Yet, the Ministry of the Interior has long struggled with a lack of personnel capacity. The occupancy of 12 systematised positions in the Cyber Security department ranged between 66% and 83% in the audited period, but at the end of the audit only 25% of positions were filled by employees who worked in the Cyber Security department for more than 3 years, despite the use of the key service position. The NCISA cannot use the institute of a key service position because Act No 234/2014 Coll., on Civil Service, does not apply to its employees, unlike those of the Ministry of the Interior. In addition, in the period 2016-2020, the Ministry of the Interior externally provided two key security roles, i.e. cyber security architect and cyber security auditor, based on contracts for the provision of consulting services in the total amount of CZK 2.25 million. This detected fact represents a risk in terms of long-term development and preservation of knowledge in the field of cyber security within the Ministry of the Interior.

Use of ESIF funds for cyber security

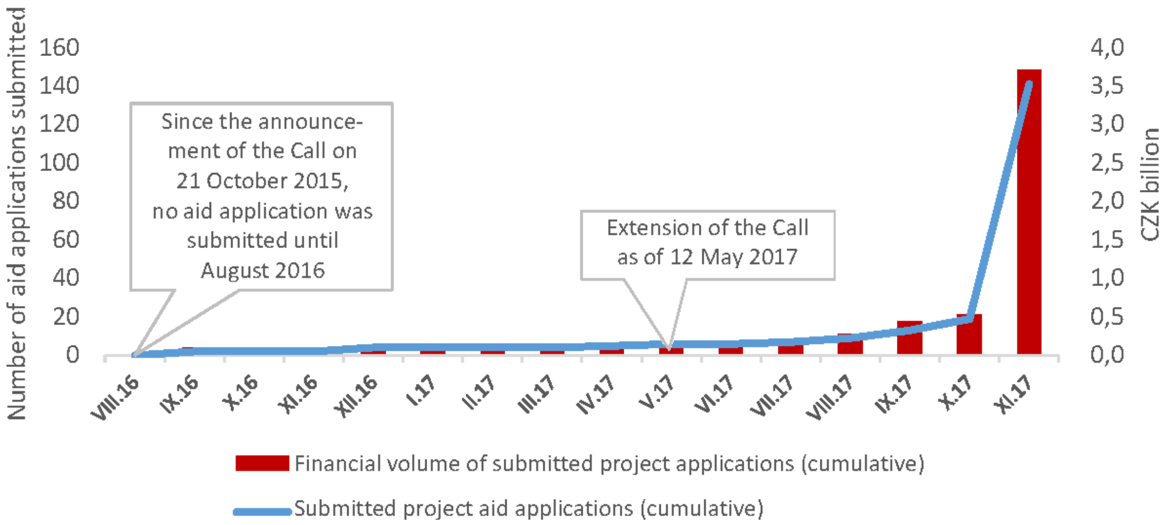
In the audited period, the ministries, the Office of the Government of the Czech Republic and other entities had the opportunity to draw funds for projects in the cyber security area within the framework of the ongoing Call No 10[18]. It was announced by the Ministry of Regional Development (MoRD) on 21 October 2015. As of the announcement date, the main supported activity was focused only on securing CIIs and MISs according to the AoCS. Nevertheless, since its announcement, Call No 10 has undergone a total of seven changes, while the change of 12 May 2017 modified, inter alia, the main supported activity. Eligible applicants could subsequently apply for funds to secure not only CIIs and MISs, but also BSIS and other information and communication systems which do not fall under the previously mentioned

[17] Cyber security is addressed at the Ministry of the Interior from a departmental point of view. From the point of view of the Ministry of the Interior, it was an issue of providing cyber security for 19 CIIs and 11 MISs.

[18] In relation to the setting of rules for drawing funds on cyber security from the ESIF, the SAO verified that MoI participated in the setting of Call No 10. The NCISA and the MoI also participate in the preparation of drawing ESIF funds on cyber security in the following programming period.

categories of systems. The total allocation of the Call amounted to approximately CZK 1,340 million (ERDF subsidy). The provision of the subsidy was subject to compliance with the cyber security standards as set out in the AoCS. The process of application filing is shown in the following chart.

Chart 2: Development of aid application submitted to Call No 10 from August 2016 to November 2017



Source: Information system *MS2014+* (data as of 24 March 2020).

The NCISA and the MoI were eligible applicants managing elements of CIIs, MISs and other information and communication systems. The NCISA used the possibility of financing under Call No 10, when it submitted two aid applications in the total amount of approximately CZK 112 million, which were subsequently approved by the MoRD. Both the projects implemented by the NCISA have already been financially completed by the MoRD. The Ministry of the Interior submitted two aid applications under Call No 10 with the required funds for their implementation in the amount of approximately CZK 368 million. Both the applications were submitted by the Ministry of the Interior in November 2017, i.e. only after the extension of the range of supported activities within Call No 10. Both the applications were excluded from the administration by the MoRD due to the high excess of aid applications above the allocation. Thus, the Ministry of the Interior did not draw any funds under Call No 10, and did not use the opportunity to finance the provision of cyber security from the allocation funds. Concurrently, the Ministry of the Interior was one of the most important OUS from the point of view of managed CIIs and MISs. In summary, funds in the amount of approximately CZK 800 million were approved by the managing authority for projects implemented by state sector entities within Call No 10. For detailed information, see the following table.

Table 2: Call No 10 - projects with approved funds for implementation

Applicants	Detailed classification of the applicant	Number of projects	Financial volume of approved aid applications (ERDF)
State sector	OUS	5	CZK 156.1 million***
	state contributory organisations	7	CZK 589.5 million*
	state enterprises	2	CZK 53.9 million
Subtotal - state sector		**14**	**CZK 799.5 million**
municipal and local authorities	regions	7	CZK 158 million
	municipalities	6	CZK 66.6 million
	organisations established or founded by regions/municipalities	27	CZK 344 million**
Subtotal - municipal and local authorities		**40**	**CZK 568.6 mil.**
State sector total + municipal and local authorities		**54**	**CZK 1 368.1 mil.**

Source: Information System *MS2014+* (data as of 24 March 2020).

* Of which 6 health care facilities projects amounting to CZK 579.1 million.

** Of which 23 health care facilities projects amounting to CZK 324.1 million.

*** Of which, CZK 121 million represented projects of central state administration bodies, where CZK 112 million went to NCISA projects.

The SAO considers it effective that the supported activity was modified, after which the eligible applicants could draw funds from Call No 10 to provide cyber security not only for CIIs and MISs, but also BSIS and other information and communication systems, which do not fall under CII, or MIS. The prerequisite was the compliance with the cyber security standards as set out in AoCS. A large part of the approved projects was submitted by health care facilities, which on the basis of valid criteria in Decree No 437/2017 Coll. do not belong to the entities managing CIIs, MISs or BSIS. Criteria for determination of BSIS in the health care sector are given in Table 3. According to these criteria, there are only sixteen health care facilities in the Czech Republic that are subject to the obligations arising from Act No 181/2014 Coll. (in all cases it is a facility managing BSIS). Cyber attacks directed against health care facilities - at the turn of 2019/2020 - showed that even if they were not mandatory entities under AoCS, a series of cyber attacks on these facilities would have a significant impact on the functionality of the Czech health care system.

Table 3: Criteria for determining BSIS in the health care sector

Sectoral criteria			Impact criteria
Type of service	**Type of entity**	**Special criteria for the type of subject**	
5.1 Provision of health care services	Provider of health care services according to the Act on Health Care Services	a) the total number of acute-care beds in the last three calendar years is at least 800 or b) the status of a centre of highly specialised trauma care according to the Act on Health Care Services	The impact of a cyber security incident in an information system or electronic communications network, the operation of which is critical for the provision of a service, may cause I. severe restriction on the type of service affecting more than 50,000 people, II. serious restriction or disruption of some other essential service or restriction or disruption of the operation of a critical infrastructure element, III. unavailability of certain type of service for more than 1,600 people, which cannot be replaced in any other way without incurring disproportionate costs, IV. casualties with a limit value of more than 100 dead or 1,000 injured people requiring medical treatment, V. breach of public safety in a significant part of the administrative district of a municipality with extended powers, which could require rescue and liquidation work by various units of the joint rescue and emergency services, or VI. may compromise sensitive personal data of more than 200,000 people.

Source: taken from Decree No 437/2017 Coll.

The SAO also audited the following three projects:

- *External Perimeter Protection* (NCISA) - examination focused on economy and effectiveness of the expended funds,
- *Cyber Security Incident Detection System in Selected Public Administration Information Systems* (NCISA) - examination focused on economy and effectiveness of the expended funds,
- eGOVMC (MoI) - examination focused on the effectiveness of the expended funds; within the project the following was audited:
  - MoI monitoring centre for the Operation of ICT Systems and Cyber Security (SOCCR),
  - first stage of construction of the NOC monitoring centre,
  - continuous development of eGOVMC.

The cost-effectiveness of the funds spent on selected projects implemented by the NCISA and financed from SB and ESIF was assessed in connection with the fulfilment of the tasks set out in AP CNCS. The audit verified whether the NCISA proceeded with the implementation of selected projects in accordance with Act No 134/2016 Coll., on Public Procurement. The effectiveness of the projects was assessed at the MoI and the NCISA in relation to the fulfilment of the approved project objectives and the objectives set out in AP CNCS. In the course of the audit of the aforementioned projects, the SAO did not detect any shortcomings that would have serious impacts on their economy and effectiveness.

As part of Audit No 19/26, the SAO performed an international comparison in the area of cyber security. For more information about the comparison, see Annex 1.

List of abbreviations

AoCS	Act No 181/2014 Coll., on Cyber Security
AP CNCS	*Action Plan for the National Cyber Security Strategy of the Czech Republic for the period from 2015 - 2020*
BSIS	*Basic service information system*
Call No 10	IROP Call No 10 - *Cyber Security*
CERT	Computer Emergency Response Team
CII	critical information infrastructure
CR	Czech Republic
CS	cyber security
CS	communication systems
eGOVMC	EGovernment Monitoring Centre
ERDF	*European Regional Development Fund*
ESIF	European Structural and Investment Funds
HW	hardware
ICT	information and communication technologies
IROP	*Integrated Regional Operational Programme*
IS	information systems
MIS	major information systems
MoI	Ministry of the Interior
MoRD	Ministry of Regional Development
NCISA	National Cyber and Information Security Agency
NSA	National Security Authority
OCA	Office of the Chief eGovernment Architect
OIK	cyber crime workplace
OUS	organisational unit of the state
PCR	Police of the Czech Republic
SAO	Supreme Audit Office
SW	software

Annex 1

International comparison

The SAO contacted the supreme auditing institutions of other EU countries in order to obtain information concerning the provision of cyber security in other countries and to compare the cyber security issues at the system level. The responses of the countries surveyed showed, inter alia, that:

- funds spent on cyber security are monitored at the state budget level only in Great Britain,
- the MIS and CII list is considered sensitive information.

The summary results of the questionnaire survey are given in the following table. The table shows that the Czech Republic has its system for ensuring cyber security set up similarly as the other countries compared. In all monitored countries, there is an entity responsible for the cyber security area, either in the form of a special state body or in the form of a ministry under the auspice of which the issue is classified. This body sets out criteria for identifying the key information systems, which are part of the legislation for most countries. The assessment of whether a given information system meets the criteria of a key system is performed either by the administrator of the given information system (i.e. the ministry, institutions) or a special cyber security body. All monitored countries have adopted the relevant strategy in order to further develop cyber security of nation-wide IS.

As described above in this Audit Conclusion, the NCISA, i.e. the State, did not have information during the audited period about the total amount of funds spent by individual chapters of the state budget on cyber security. Most of the countries under comparison have a system of securing cyber security and its development that is similar to the one employed in the Czech Republic. It is worth mentioning the different approach to the reporting of funds for the provision and development of cyber security in Great Britain. Great Britain reports funds for the provision and development of national cyber security at the level of a special budget item. Therefore, Great Britain can better monitor the amount of funds that are spent on cyber security at the level of the entire state.

Summary of the results of the questionnaire survey

	Czech Republic	Latvia	Germany	Great Britain	Cyprus	Finland
Existence of criteria for determining the key IS	**YES**	**YES**	**YES**	**NO**	**YES**	**YES**
Legal regulation of criteria	**Act** (on Cyber Security), **decree**	**Act**	**Act** (on Cyber Security), **decree**	**Other methodological material**	**Act** (general criteria), **other methodological material** (detailed criteria)	**Act, other methodological material**
Authority responsible for cyber security	**Special body for cyber security** (NCISA)	**Ministry** (of defence, responsible for cyber security)	**Ministry** (Federal Ministry of the Interior, Building and Community)	**Ministry** (Office of the Government, Centre for National Infrastructure Protection)	**Special body for cyber security** (Digital Security Office)	**Ministry** (of finance, responsible for cyber security)
A body assessing the fulfilment of critical IS criteria	**IS administrator**, the results are transmitted by NCISA (it will put major IS and basic services on the relevant list and in the case of critical IS it will request the inclusion in the list of critical infrastructure)	**IS administrator**, for critical IS, the administrator or the security office (the proposal will be assessed by an intergovernmental commission for national security and submitted to the government for approval)	**IS administrator** (if IS is evaluated as critical, the administrator shall contact the Office for Information Security)	Unknown to the respondent	**Special body for cyber security** (Digital Security Office)	**Special body for cyber security** (National centre for cyber security)
Number of public IS, of which critical	8 000 • 45 critical, • 178 major, • 30 providers of basic services	The total number of IS is unknown, the number of critical IS is restrictedinformation	The total number of IS cannot be quantified, 1,500 critical IS, 600 critical infrastructure operators	The information is not in the public domain	Data on the total number of IS not specified, 50 critical IS + others in the semi-state sector	4,000 IS in the public sector

	Czech Republic	Latvia	Germany	Great Britain	Cyprus	Finland
					(government-owned organizations)	
Financing the provision of national cyber security	**At the level of the IS administrator** (there is no special budget item, therefore it is not possible to quantify the planned costs for cyber security)	**At the level of the IS administrator** (there is no special budget item, therefore it is not possible to quantify the planned costs for cyber security); **at the level of a special cyber security body**	**At the level of the IS administrator** (**usually** there is no special budget item, therefore it is **usually** not possible to quantify the planned costs for cyber security)	**At the level of the state budget** (special budget item)	**At the level of the IS administrator** (the respondent does not provide details, but due to the impossibility to quantify the costs in the following question, it can be assumed that there is no separate budget item)	**At the level of the IS administrator** (there is no special budget item, therefore it is not possible to quantify the planned costs for cyber security)
Costs of cyber security 2015-2020	**Cannot be determined** (due to the method of cost planning, see above)	**Cannot be determined** (due to the method of cost planning, see above)	**Cannot be determined** (due to the method of cost planning, see above)	GBP 1.3 billion (2016-21)	**Cannot be determined** (due to the method of cost planning, see above)	**Cannot be determined** (due to the method of cost planning, see above). Solution in progress. Possible improvement in the future
Strategy for development of cyber security	**YES** (2015-20), issued by a special body for cyber security + action plan	**YES** (2019-22), prepared by the MoD responsible for cyber security, approved by the government + action plan	**YES** (2016)	**YES** (2016-21)	**YES** (2012), issued by special body for cyber security	**YES** (2019), a more detailed implementation plan is envisaged

Source: prepared by the SAO based on the answers of audit institutions.