NATIONAL SECURITY AUTHORITY

Annual Report

2019

TABLE OF CONTENTS

1. ORGANISATION IDENTIFICATION

NAME	National Security Authority
REGISTERED OFFICE	Budatínska 30, 851 06 Bratislava
TYPE	Central government authority
STATUTORY BODY	JUDr. Roman Konečný, director
ESTABLISHED ON	1 November 2001
CONTACT	+421 2 6869 1111, podatelna@nbu.gov.sk
WEBSITE	www.nbu.gov.sk

MAIN ACTIVITIES

The National Security Authority (hereinafter referred to as the "Authority") is responsible for the creation and implementation of the state policy for the field of protecting classified information, cryptographic service, trust services, and cybersecurity. In each area, it carries out activities that help to achieve the Authority's objectives.

In the field of protection of classified information, the Authority performs security clearance of individuals and entrepreneurs, expresses its opinion on individuals under international treaties by which the Slovak Republic is bound and keeps the register related to the protection of classified information. Furthermore, it carries out accreditation of communication and information systems for handling of classified information, gives authorisation to state bodies or authorisation to entrepreneurs for certification of technical device and verification of conformity of mechanical barrier devices and technical protection devices with security standards and carries out certification of technical, system, mechanical barrier and technical protection devices. The Authority performs assessment of conditions at entrepreneurs and state bodies, including the assessment of ensuring protection of exchanged classified documents and assessment of conditions for protection against undesirable electromagnetic radiation. In its own capacity the Authority conducts inspection of conditions ensuring protection of classified information in state, municipal bodies and at entrepreneurs, and publishes methodological guidelines for individual aspects of classified information security. It further performs activities strengthening security awareness and conducts security officer's examinations. Within international exchange of classified information, the Authority performs the role of central registry of classified information in Slovak Republic and participates in the protection of classified information of other countries.

In the field of cryptographic protection of information (CPI) the Authority performs certification of CPI devices, publishes security standards and conducts research and development of CPI devices. It serves as guarantor and national authority within international cooperation in the field of CPI and provides the function of National distribution authority, which is the entry and contact point in the Slovak Republic for exchange and distribution of cryptographic material and cryptographic devices.

In the field of trust services, the Authority performs the task of supervisory authority in the Slovak Republic. It conducts tasks related to certification of devices for production of qualified electronic signatures and qualified electronic stamps; creates, manages and publishes a trusted list and list of authorisations for the purpose of issuing mandate certificates. It operates the Root Certification Authority in the Slovak Republic issuing certificates of public keys to qualified providers of trust services. Until 31 July, the Authority also operated the Slovak National Certification Authority (SNCA), which is the qualified provider of trust services for public authorities. From 1 August 2019, the services of SNCA are provided by the National agency for Network and Electronic services.

In the field of cybersecurity, the Authority is the national authority for cybersecurity. It manages and coordinates the performance of government authorities in the field of cybersecurity, sets standards and issues behavioural policies for cyberspace. The Authority is the primary contact point for foreign countries in the area of cybersecurity, cooperates with central authorities, providers of basic services and digital service providers, it also performs the task of national unit CSIRT (Computer Security Incident Response Team).

KEY LEGAL REGULATIONS

In the accomplishment of set tasks, the Authority is governed by the Constitution of the Slovak Republic, constitutional acts, legally binding acts of the European Union, international treaties that the Slovak Republic is bound by, acts and other generally binding legal regulations, resolutions of the Government of the Slovak Republic, its statute, establishment plan and other internal legal regulations setting forth the internal processes.

In performance of set tasks in the field of classified information protection and cryptographic protection of information, the Authority is regulated by Act on Protection of Classified Information (Act No. 215/2004 Coll. on Protection of Classified Information and on amending and supplementing certain acts as amended). In the field product certification for trust services, the Authority follows the eIDAS Regulation (Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market), it's implementing decisions are regulated by Act on Trust Services (Act No. 272/2016 Coll. on Trust Services for electronic transactions on the internal market and on amending and supplementing certain acts). In performance of tasks in the field of cybersecurity, the Authority is regulated by Cybersecurity Act (Act No. 69/2018 Coll. on Cybersecurity and on amending and supplementing certain acts).

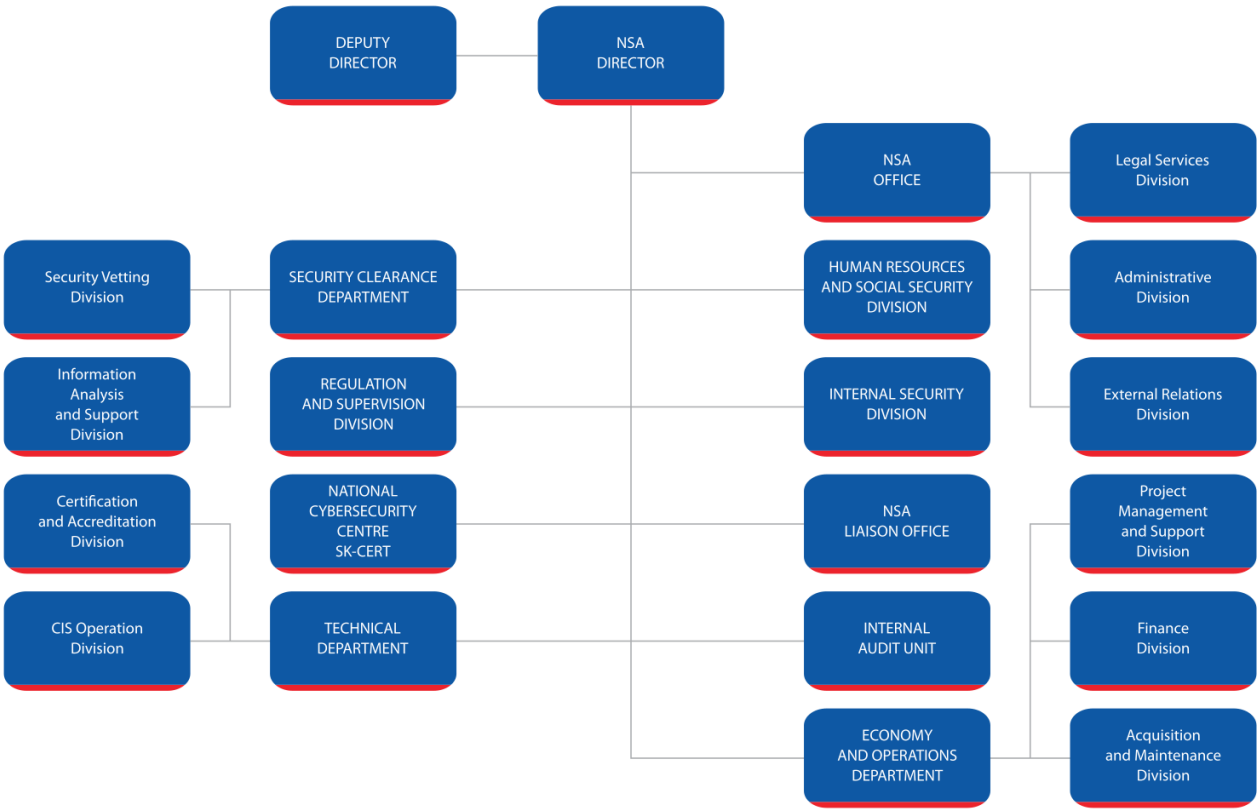
LEADERSHIP OF THE AUTHORITY

The Authority is headed by the Director, who is responsible for the activity of the Authority. He manages and represents the Authority outwardly. The Director decides on the method of implementation of the main tasks of the Authority, approves the internal legal regulations, and decides on the internal organisational structure of the Authority and on the personnel issues of its officers and employees. He covers the interdepartmental cooperation of the Authority and is a permanent member of the Security Council of the Slovak Republic. He determines the principles of international cooperation of the Authority and in compliance with the foreign policy priorities of the Government of the Slovak Republic, supports and develops partnerships with institutions of foreign states and international organisations. In his absence, the director is in a reserved scope represented by the Deputy Director of the Authority, who is also responsible for coordination of the activities of units.

ORGANISATIONAL STRUCTURE

The organisation of the Authority is divided into departments – sections and directly managed divisions, sections are further divided into divisions.

Internal structure of the Authority as of 31 December 2019:



UNITS OF THE AUTHORITY

The Security clearance department in the field of personnel security and industrial carries out tasks related to execution of security clearance for individuals and entrepreneurs. Apart from security certificates and confirmations, which allow access to national classified information, it also conducts issuing of personnel security clearance certificates and facility security clearance certificates for handling of classified information of NATO and EU; performs security clearance for individuals and entrepreneurs, issues certificates for access to classified information of NATO and EU, expresses its opinion on individuals under international treaties by which the Slovak Republic is bound.

The **Regulation and Supervision Division** is a subject unit handling areas of classified information, cryptographic protection of information, cybersecurity, trust services and public regulated service, which is provided by satellite navigation system project Galileo. It fulfils tasks in areas of inspection, audit and supervision. It issues and revokes qualifying status, determines basic service and its provider, determines digital service and its provider. Issues official statements and methodologies, creates conceptions and strategic materials, prepares security standards and knowledge standards, certification policies and signature policies, behavioural policies in cyberspace, principles of cyber incident prevention and methods of their resolution. On the international level it represents the Authority and coordinates international activities of the Authority. It comments the proposals of legislative materials in the interdepartmental consultation procedure and carries out the legal process of materials with foreign elements.

The **National Cybersecurity Centre SK-CERT** carries out duties of national unit CSIRT. It ensures services related to managing security incidents, removing their impacts and consecutive restoration of operation of information systems in cooperation with their owners and providers. It also performs analytical tasks, research, raising security awareness and education in fields of cybersecurity and other duties in the field of cybersecurity.

The **Technical Department** carries out accreditation and certification in the area of protection of classified information for personnel security, security of information, physical security and facility security, security of technical devices and industrial security, in the area of cryptographic protection of information, cybersecurity and trust services. It maintains the course and operation of information and communication systems of the Authority.

The **NSA Office** coordinates the activity of the Authority units, secures and performs basic administrative and organisational activities related to management and activities of the Authority, arranges legislative and legal matters of the Authority, builds and develops external relationships and cooperation, and ensures communication to the public.

The **Human Resources and Social Security Division** carries out personnel and wage policy, social security, education and payroll. It coordinates healthcare for officers and employees of the Authority.

The **Internal Security Division** ensures internal security of the Authority and provides for physical and technical protection of the Authority´s facility. It performs internal oversight and handles complaints and petitions. It fulfils tasks of responsible entity for handling reports of antisocial activity in the field of protection of personal information; prepares agreements about entrepreneur's access to classified information and performs duties in occupational safety and health (OSH) and fire protection.

The **NSA Liaison office** fulfils specific tasks in developing and building international relations and cooperation of the Authority abroad. The office provides communication between the Authority and foreign partners, represents the interests of the Slovak Republic in areas entrusted to the Authority within NATO, European institutions and agencies, and implements bilateral and multilateral cooperation within the Authority's representation abroad.

The **Internal Auditor** performs internal audit of the Authority and performs other tasks under the financial audit act.

The **Economy and Operations Ddepartment** secures financial management of the Authority, coordination in the process of management of funds, including accounting and reporting, management and maintenance of assets, public procurement for the needs of the Authority and participates in coordination of project and program management and projects financed by EU sources.

2. HUMAN RESOURCES

Officers work at the Authority in civil service pursuant to Act No. 73/1998 Coll. on Civil Service of the Members of the Police Force, Slovak Information Service, Prison and Court Guards Service and Railway Police Force and employees in employment relationship pursuant to Act No. 552/2003 Coll. on Performance of Work in Public Interest.

ANTI-CORRUPTION PROGRAM

In 2019 the Authority developed its own **anti-corruption** program, which is based on the anti-corruption policy of the Slovak Republic for year 2019-2023 from December 2018. It addresses in detail the government anti-corruption policy and projects it into the environment of the Authority. The authority anti-corruption program is a tool **for strengthening and asserting anti-corruption culture**, and improving corruption risk detection and management. In it the Authority assesses the existing corruption risks and establishes specific systemic measures aimed at prevention of corruption and support of anti-corruption behaviour of its employees.

ETHICAL CODEX

In autumn 2019 the ethical codex was formulated, which sets the **rules for maintaining honest, proper, socially responsible, professional and moral principles** for staff of the Authority. This applies not only in interpersonal communication, but also in relations in the eternal environment. The ethical codex clarifies policy in sensitive matters of the authority and expresses an effort to work and manage with the highest principles of personal etiquette.

Together with the Anti-corruption program, the ethical codex represents a tool of positive motivation for staff of the Authority, which strengthens the sense that they are working in an ethical environment with clear rules applicable to everyone. The codex applies to all staff of the Authority, regardless of their work assignment, position or hierarchy of command. Sanctions for violation of the set ethical principles are imposed by the Ethical commission of the Authority. In the year 2019 there were no inputs submitted to the commission for violating the principles of the ethical codex by members of the staff.

STATISTICAL INDICATORS

The total number of staff of the Authority in the last three years was relatively stable. The ratio between officers and employees has not changed significantly (approx. 90:10), the slight prevalence of the number of women over the number of men was also maintained. The data as of 31 December of the particular year are described in Table No. 1.

Table No. 1: Number of officers and employees in years 2017 – 2019

	31.12.2017	31.12. 2018	31.12. 2019
Officers	**197 (90,78%)**	**200 (89,69%)**	**195 (89,45%)**
in preparatory civil service	19 (9,64%)	18 (9,00%)	12 (6,15%)
in permanent civil service	177 (89,85%)	179 (89,50%)	180 (92,31%)
in temporary civil service	1 (0,51%)	3 (1,50%)	3 (1,54%)
Employees	**20 (9,22%)**	**23 (10,31%)**	**23 (10,55%)**
Total	**217** (115 women a 102 men)	**223** (119 women a 104 men)	**218** (118 women a 100 men)

In year 2020 the trend of strengthening the most numerous age group of 35 to 49 was maintained. In year 2019 the members of this group made up among the officers a total of 62,05% (26,09% among employees). This group is comprised of mostly experienced professionals with several years of experience in the most productive age range. All data about the age structure of the Authority is available in Table No. 2.

Table No. 2: Age of officers and employees of the Authority in years 2017 - 2019

	31.12.2017		31.12.2018		31.12.2019	
	Officers	Employees	Officers	Employees	Officers	Employees
	197 (100%)	**20** (100%)	**200** (100%)	**23** (100%)	**195** (100%)	**23** (100%)
Younger than 34 years	**39** (19,80%)	**1** (5,00%)	**38** (19,00%)	**6** (26,09%)	**35** (17,95%)	**6** (26,09%)
35 to 49 years	**117** (59,39%)	**2** (10,00%)	**121** (60,50%)	**3** (13,04%)	**121** (62,05%)	**6** (26,09%)
50 to 59 years	**32** (16,24%)	**10** (50,00%)	**35** (17,50%)	**7** (30,43%)	**32** (16,41%)	**6** (26,09%)
Older than 60 years	**9** (4,57%)	**7** (35,00%)	**6** (3,00%)	**7** (30,43%)	**7** (3,59%)	**5** (21,74%)

DEEPENING OF QUALIFICATION AND INCREASING OF SKILLS

The Authority enables its officers and employees to maintain their professional preparedness, gain new skills and increase their qualification in professional courses, seminars and training sessions domestically and abroad. If required, the Authority secures increasing of qualification at universities. Every year it organises a specialised police education for newly hired officers, in cooperation with the Academy of the Police Force in Bratislava, which is a condition for inclusion of the newly hired officers in permanent civil service. The data on the education structure of officers and employees of the Authority is included in Table No. 3.

Table No. 3: Education of officers and employees of the Authority in years 2017 – 2019

	31.12.2017		31.12.2018		31.12.2019	
	Officers	Employees	Officers	Employees	Officers	Employees
	197 (100%)	**20** (100%)	**200** (100%)	**23** (100%)	**195** (100%)	**23** (100%)
Basic	**0** (0,00%)	**2** (10,00%)	**0** (0,00%)	**2** (8,70%)	**0** (0,00%)	**2** (8,70%)
Full secondary	**30** (15,23%)	**12** (60,00%)	**32** (16,00%)	**12** (52,17%)	**29** (14,87%)	**12** (52,17%)
University – Level I	**4** (2,03%)	**0** (0,00%)	**5** (2,50%)	**1** (4,35%)	**6** (3,08%)	**0** (0,00%)
University – Level II	**154** (78,17%)	**6** (30,00%)	**152** (76,00%)	**7** (30,43%)	**150** (76,92%)	**8** (34,78%)
University – Level III	**9** (4,57%)	**0** (0,00%)	**11** (5,50%)	**1** (4,35%)	**10** (5,13%)	**1** (4,35%)

In addition to periodic OSH and fire protection trainings, other internal education sessions were organized in year 2019. These were focused on the practical application of internal legal regulations, the application of personnel and disciplinary powers of superiors and compliance with the regime measures of the Authority facility. The Authority secured access for selected officers, who are assigned to fulfilling tasks related to facility protection and personnel protection, at a special preparation at the Military training centre of Ministry of Defence of the Slovak Republic at Lešť. With the goal of achieving required physical fitness levels of Authority staff, the material equipment of the gym was expanded in 2019. The gym is accessible to all Authority staff, which supports maintaining and increasing physical condition and vitality.

3. FIELDS OF ACTIVITY

In the process of task fulfilment, the Authority takes into consideration the legal framework determining its activities. The completion of designated tasks involves a number of executive, but also legislative, administrative and other support activities.

3.1 LEGISLATION

The Authority has reacted to the developments in the security environment in 2019, especially to the rapid informatization of society and the growing dynamics of security threats **by drafting legislative proposals** and introducing suitable legislative conditions, which were a necessary reaction to the growth trends and issues coming from their application.

GENERALLY BINDING LEGAL REGULATIONS

The **new legislation in the field of protection of classified information** was in preparation process throughout 2019, its goal was to set optimal principles and minimal standards for the creation of a secure environment for classified information. The year 2019 was a transition period, which preceded the **Decree on security of information** (NSA Decree No. 48/2019, which establishes the specifics of security of classified information). The goal of setting a one year transition period of the decree coming into force, which has a significant impact on current philosophy in this field, was to provide individuals and legal persons a sufficient timeframe to acquaint themselves with the changes in this strictly regulated field before 1 January 2020. The Authority also used the deadline to organise a series of presentations, methodological days and bilateral expert meetings with representatives of the most exponential public authorities and entrepreneurs.

On 1 September 2019, the **Amendment to the Act against Bureaucracy** (No. 221/2019 Coll.), which also amended and updated the Act on protection of classified information: specifically by issuing a new security questionnaire for entrepreneurs. In line with the philosophy of the anti-bureaucratic act, entrepreneurs were exempt from responsibility of providing the Authority with information, which it can acquire from existing state registries or in cooperation with other state bodies when requesting their facility security clearance.

On 19 June 2019, **Act No. 211/2019 Coll.** was declared in the Collection of Laws of the Slovak Republic, which amends and supplements Act No. 305/2013 Coll. **on Electronic Form of Exercise of Powers by Public Authorities** and on amending and supplementing certain acts (Act on e-Government) as amended, i. a. Act on trust services.

On 1 January 2019, **Decree No. 362/2018 Coll. on Determining the Content of the Security Measures**, content and structure of security documentation and the scope of general security measures came into force. In August 2019, the Authority submitted into interdepartmental consultation an initiative **draft proposal of Decree on Cyber Security Audit and Auditor's Knowledge Standard**. After it passed the national legislative process, the decree was issued on 11 December 2019 in the Collection of Laws under No. 436/2019 Coll. (coming into force from 1 January 2020). It is the fifth implementing regulation for the Cybersecurity Act.

INTERNAL REGULATIONS

In year 2019 the Authority issued **12 regulations** of the Authority director, **32 orders** of the Authority director **and three statutes**. The regulations and statues were issued with the goal of **increasing the effectiveness of internal processes**, **implement generally binding legal regulations** (e.g. new regulation on public procurement, on appeal commission, new registry order, Ethical codex, amendment of the organisational order, amendment of personnel records and tasks of the Authority units related to the civil service of officers, new **statute on internal audit** and a new **status of the National Incident Response Unit SK-CERT**). The order of the Authority director served to designate the holders of specific tasks – e.g. training, asset inventory, delimitation of assets and establishment of project teams.

ADMINISTRATIVE AND INFRINGEMENT PROCEDURE

In 2019 the Authority received **eight complaints for unauthorised handling** of classified information. The Authority, as administrative authority for this field issued fines in total amount of 300 Euro. The Authority also dealt with **five complaints** to initiate administrative proceedings on the matter of **violation of the Act on Trust Services**. The proceedings were suspended in all cases. The Authority received **five submissions in the section of areal photography**. All submissions were postponed and filed by the Authority, as no misdemeanors were identified as per the Act on Protection of Classified Information.

EXPERT ACTIVITY

The Authority is an **expert organisation** registered in the list of experts, maintained by the Ministry of Justice of the Slovak Republic in the field 520000 - protection of classified information. In 2019, the respective authorities did not apply to the Authority for expert assessment.

3.2 INTERNATIONAL RELATIONS

In 2019, **the Authority cooperated with EU and NATO security authorities** and other international organisations in all areas of its competence. The Authority has taken active steps to **promote regional cooperation and the development of bilateral partnerships** enabling the exchange of experience, the formulation of uniform positions and the coordination of practices in promoting common interests. Through the Central Register site, the Authority provided an **international exchange of classified information** and was involved in protecting it.

ACTING IN THE BODIES OF THE EUROPEAN UNION

The Authority shall have expert representation in all three platforms of EU bodies and institutions dealing with **security and security policy of the EU (EUCI)**. At the heart of the 2019 EUCI-related agenda were the development of security policies focused on industrial security, **the Council's** security regulations and **the EEAS**, the draft rules on security of **the Court of Justice and the General Court**, as well as **cooperation between EU institutions, agencies, offices and bodies** in protecting EUCI.

At **the European Commission** in 2019, a great deal of attention was paid to the security framework of **the European Defence Industries Development Programme.** Members of the Authority also participated in the meetings of **the Security Policy Expert Group (ComSEG)**, which is responsible for the preparation and implementation of security policies and rules in the spectrum of EU institutions. Other EC formats involving representatives of the Authority are t**he Global Navigation Satellite System Expert Security Committee (GNSS SB)** and **the European GNSS Agency Security Accreditation Panel (GSA)** in the framework of the development of the Galileo satellite system (SAB).

The European External Action Service (EEAS) shall act as the EEAS Security Committee for the preparation of policies and proposals (security in general), the protection of classified information under the terms and conditions of the EEAS and its foreign delegations, as well as the updating of international agreements in the EUCI area, including the Office's delegated representatives. The Authority's experts also participated in meetings of the EEAS Subcommittee (SAB) – EEAS Subcommittee on Security Accreditation EU OPS WAN.

The Council of the EU paid attention to the use of **cryptographic information protection assets** to protect EUCI under Member State conditions, in particular in relation to EU-led missions and operations. Members of the Authority regularly participated in **the Security Committee of the EU Council (CSC)**, where they addressed issues related to protection against undesirable electromagnetic radiation in **the TEMPEST Implementation Task Force (ITTF).**

A number of important EU legal acts were adopted in 2019 to **strengthen the fight against cyber threats**, the most important of which are the **ENISA Regulation** (Regulation (EU) 2019/881 on the European Union Cybersecurity Agency ENISA) and on the certification of cybersecurity of information and communication technologies and repealing Regulation (EU) No 526/2013 (the Cybersecurity Act) which entered into force on 7 May 2019. Following the effectiveness of this legislation, **the European Cybersecurity Certification Group ECCG** was established, in which the Slovak Republic is represented by the Authority. The ECCG is based on the principles and procedures of the Common Criteria Recognition Arrangement (CCRA). At the same time as the grouping was involved, the Authority for the Slovak Republic joined the CCRA.

The Slovak Republic, through the Authority, strengthened and deepened its cooperation with **ENISA** in 2019, which, in its position as a Cybersecurity Centre in the EU, helps Member States to be better equipped and prepared to prevent, detect and solve cybersecurity problems. The cooperation involved the coordination of responses to global cyber incidents and also covered a share in the implementation of ENISA's activities, commenting on decisions and representation of the Director of the National Cyber Security Centre SK-CERT in ENISA's **Management Board.** In 2019, the head of the special foreign office was appointed as an alternate for the Slovak Republic.

In view of the obligation of Member States to transpose the NIS Directive into national legislation, continuous dialogue was still needed in 2019. In particular, emphasis has been placed on addressing issues related to the identification of operators of basic services. **The NIS Cooperation Group and the Computer Security Incidents Team (CSIRT's Network)** held an active position in this process. The main task of these working platforms was to ensure and intensify strategic and operational mutual cooperation, to share information between Member States 'cybersecurity authorities and between their CSIRTs. The platforms worked on a periodic basis and adopted the necessary rules and procedures. Key priorities for the work of the group and the role of the CSIRT network for ensuring EU operational capabilities have been defined, as well as a joint coordinated EU response to cyber security incidents and large-scale crises.

In the second half of 2018, the EC proposed legal instruments to implement the EU's empowerment initiative that would enable it to become a global leader in cybersecurity, to ensure trust, reliability and protection of citizens, consumers and businesses online, and to enable a free and legal internet. A proposal for a European regulation to establish a **European Centre for Sectoral, Technological and Research Competences in Cyber Security and the Network of National Coordination Centres** is put forward in the legislative process. The text was debated throughout 2019 in the working format of the Council of the EU and debated in the legislative process.

Working format **The Horizontal Working Group on Cyber Affairs (HWP)** addressed cross-cutting cyber issues affecting cyber threat assessment, cybercrime, cyber diplomacy and certification. Over the reporting period, the topics dominated by the reform of the WHOIS domain name database, the implementation of the framework for a common EU diplomatic response to harmful cyber activities, and the distribution (attribution) of harmful cyber activities and the possibility of introducing a framework of restrictive measures to respond to or deter cyber threats. In 2019, a **Council Regulation and Council Decision on restrictive measures against cyber attacks threatening the Union or its Member States were prepared** (and approved at ministerial level) on the work plane of HWP.

The main non-legislative theme in the EU in 2019 was **the fifth generation cybersecurity (5G)** cybersecurity theme. In cooperation with public authorities, telecoms regulators and telecoms operators, in the context of the EC Cybersecurity Recommendation 5G Networks of March 2019, the Authority carried out a national risk assessment of the implementation of 5G technologies, which was the basis for **the Joint European Risk Assessment of 5G Networks** issued in October 2019. In early 2020, EU Member States, with the support of the EC and ENISA, published **a 5G Toolbox to address cybersecurity risks of 5G networks**. Member States should implement the individual measures in a further sequence and, by 1 October 2020, should assess the impacts and determine whether further action will be needed, in cooperation with the EC.

Throughout 2019, the Authority was also active in **the European Organisation for Cyber Security (ECSO)**. In the organisational structure of ECSO, the Authority is a member of the Committee of Representatives of National Public Authorities (NAPAC) and an observer on the Board of Directors. The representatives of the Office participated in the work of three of the six WG1 working groups: Certification, standardisation, WG5: Cybersecurity education, security awareness building and training, WG6: Strategic research and innovation agenda.

ACTING IN THE BODIES OF THE NORTH ATLANTIC TREATY ORGANISATION

The Authority was actively involved in the regular spring and autumn meetings of **the NATO Security Committee (SC)** at the level of the Heads of Security Authorities of the Member States and at the level of the development of security policies. The Committee addresses all issues related to the Alliance's security policy and is an advisory body to the North Atlantic Council (NAC).

In the Security Committee for Security Policymaking, the Authority's representatives participated in a comprehensive review of C-M(2002)49 (NATO security policy) and its complementary directives for all security areas. The novelty was the introduction of **two new directives**, which covered **all aspects of the protection of NATO classified information** in relation to non-member entities as a requirement resulting from the application practice of NATO military and civilian components. One of the largest SC meetings on cooperation aspects with non-member countries took place in Warsaw in May 2019.

In the context of developments in the security environment and the recognition of cyberspace as the operational domain of NATO (Warsaw Summit 2016) the issue of cybersecurity is increasingly becoming a priority for NATO authorities. The conclusions of the 2019 London Summit confirmed that cyber threats to NATO are becoming more frequent, complex and destructive. In February 2019, the Member States approved a NATO Handbook **defining tools to strengthen the Alliance's capability to respond to major cyber incidents**. Work continued on the creation of the **Cyber Operations Centre** to become part of the reinforced NATO command structure. Through its representative, the Authority worked in the **Cyber Defence Committee (CDC)**, which is the overarching political body for cyber defence of the Alliance and participated in the preparation of NATO's cybersecurity strategy papers.

The Authority at national level covered the 12nd edition of the **Cyber Coalition 2019**, which was traditionally held in Estonia. The exercise was aimed at verifying national capabilities and procedures according to NATO's existing legislative rules and procedures, as well as promoting better coordination and cooperation between sectors. The Authority was also active in the **MN MISP** (Multinational Malware Information Sharing Platform) platform, which enables informal exchange of information on cyber threats between 27 NATO member states and six NATO partner countries.

In 2019, the Authority served in **the NATO Security Committee** in the format for communication and information systems SC (CISS) and t**he NATO Subcommittee on Information Security and Cyber Protection (CaP4)**. In the structures of **the BICES** (Battlefield Information Collection and Exploitation System), the Authority members participated in t**he BSWG Security Working Group** (BICES Working Group) and **the BSAB Security Accreditation Board** (BICES Accreditation Board). They also participated in the work of **the NATO Security Committee on Information Assurance** (CISS), **the NATO Security Accreditation Board** (NATO Security Accreditation Board) and **the Specifications for Interoperability for Key Management (NATO-KM-ISPEC)**.

In 2019, the Authority cooperated in replying to the NATO questionnaire on **defence planning capabilities**. The Slovak Republic is obliged to complete a questionnaire once every two years and to measure progress in individual areas. The Authority participated in the areas of cyber defence and civilian planning. In October 2019, members of the Authority took part in negotiations with NATO to answer supplementary questions. The evaluation will be known in spring 2020.

In 2019, members of the Authority participated in the **NATO crisis management exercise CMX** (at the highest strategic level to exercise and improve political consultation and decision-making) in the implementation of the **National Crisis Response System measures**. The Authority was involved in the management, coordination, monitoring and evaluation of the exercise in the national management staff.

The Authority also participated in a joint **NATO Able Staff 2019** alliance exercise to test communication procedures related to nuclear planning, to train usable measures of the Alliance's crisis response system, to bring improvements in the consultation area, to implement practical training of personnel at NATO headquarters, the Headquarters of Allied Forces in Europe (SHAPE) and national headquarters. The Authority participated in the exercise at distribution level, ensuring that classified information was received and transmitted through the Central Registry Office. Communication during the exercise took place through the NNCCRS (NATO Nuclear Command Control Response System) information system, which circulated the flow of information between the relevant departments, office and NATO headquarters.

The Authority also operates in the **Multinational Industrial Security Working Group (MISWG)** to adapt security procedures in a constantly evolving security environment and to take into account changing trends in the defence industry and international industrial security. It consists of member states of NATO (except Iceland) but also a number of non-members (Austria, Finland, Sweden, Switzerland, Israel, New Zealand, Australia and Northern Macedonia). The Group shall establish common measures and procedures for the protection of classified information relating to international defence programmes and industrial security matters in an international context. In September 2019, the 34th MISWG plenary session was held under the auspices of the Croatian Presidency in Split, which provided a platform to exchange and share the experience of representatives of the partner security authorities in carrying out business security clearances, evaluating security risks and eliminating them. Participants in the MISWG split meeting decided to accept Montenegro as a full member of the organisation.

WORKING IN THE ORGANISATION FOR SECURITY AND COOPERATION IN EUROPE

The Authority is the only official technical point of contact of the Slovak Republic in **the Organisation for Security and Cooperation in Europe (OSCE)** for cybersecurity. It is active in the informal Cyber Issues Working Group and actively participates in the common objectives set. In 2019, the Slovak Republic chaired the OSCE. In March, the Presidency organised the annual **Vienna Cyber Security Week** in cooperation with the EnergyPact Foundation. In June 2019, the Slovak OSCE Presidency organised a two-day international conference on **Safer Cyber/ICT in Bratislava: The role of the OSCE in promoting regional cybersecurity,** addressing topics related to ICT security and cyberspace security.

REGIONAL COOPERATION

The Authority's important priorities in 2019 included strengthening regional cooperation as part of the Authority's broader interest in building quality international relations. This kind of cooperation serves to exchange the experience and views of the associated countries, but above all to seek common consensus and support in the development of European legislation. In 2019, the Authority continued to develop well-established and functioning relations with strategic partners from the Visegrad Four and Austria countries. The effect of cooperation in the Central European region was confirmed in particular within the informal **Central European Platform on Cyber Security** (CECSP). It once again succeeded in finding common and unifying views on current European issues. The annual meeting of the Platform was held by the Austrian Presidency in Vienna in October 2019. The main topics of the meeting were the implementation of the NIS Directive, the security of 5G networks, the certification of cyber security and the proposal to establish a European Centre for Sectoral, Technological and Research Competences in the area of cybersecurity and a network of national coordination centres. The importance of the format and topicality of the cybersecurity topic in the Central European Area was particularly highlighted at the meeting. In 2020, the platform is chaired by Hungary.

BILATERAL PARTNERSHIPS

In 2019, the Authority was active in the process of **implementing bilateral agreements on the exchange and protection of classified information**, without which the international exchange of classified information could not take place, the recognition of security clearances issued abroad and the private sector would not be able to participate in the execution of contracts involving foreign classified information. As the responsible authority, the Authority addresses its partners abroad and prepares draft texts of agreements approved by the Government of the Slovak Republic.

In 2019, the Authority's bilateral relations with Czech partners from t**he National Bureau of Cyber and Information Security (NÚKIB)** and **the National Security Authority (NBU)** were intensified. In addition to regular bilateral meetings of the Director of the Office with Czech partners, several working discussions were organised in Prague, Brno and Bratislava on issues of methodology and law in the field of cybersecurity, practical experience from the implementation of the NIS Directive into national legislation. They also focused on the exchange of state-of-the-art knowledge on application practices in the field of adverse electromagnetic radiation protection and information on the approaches applied in the field of information encryption.

In 2019, the Authority continued to develop bilateral strategic partnerships, in particular in the field of cybersecurity. He continued his dialogue with representatives of the French **National Agency for Cyber Security (ANSSI)**. The dialogue was supported by bilateral working meetings in Paris, Lille, The Hague and Brussels. This resulted in consultation of opinions, exchange of experience and views, which, if a consensus was found, led to mutual support in European policy-making (legislative process, 5G, attribution process, etc.).

The Authority continued to cooperate with **the Federal Bureau of Information Security (BSI)**, which is also the federal authority for cybersecurity. In addition to the exchange of experience at bilateral workshops, the Authority and the BSI were at the birth of the newly emerging format of regular meetings of the Heads of National Cyber Authorities, which aims to create a space for the exchange of strategic information at the highest level of governance.

In 2019, the Authority continued to work with an **American partner**. Talks on a new bilateral agreement on mutual exchange and protection of classified information between the Slovak Republic and the US were renewed. Further cooperation on cyber security has been deepened. With regard to Brexit, a dialogue has been launched with a **British cybersecurity partner** at the Foreign Ministry in London. The first workshops on topical European themes were held to find an effective way of further communication after Great Britain's departure from the EU.

The international empowerment of the Authority, which is also linked to the operation of a Special Foreign Office in Brussels, has also made it possible to respond promptly to the EU's request to provide assistance to partner countries in the field of cybersecurity. Such an example is **active cooperation in closer formats**, for example in the V4 format, as well as in bilateral cooperation with individual countries (Finland and Romania) at EU level in Brussels. The Authority was also actively involved in the EU-China, EU-Japan, EU-Ukraine, EU-Ukraine European Dialogues through a dedicated site. The countries presented their cybersecurity systems and their willingness to develop cooperation with the EU and its Member States.

In 2019, the Authority participated in professional formats focused on the cybersecurity of the banking sector, where, at the invitation of Dutch National Bank of the Netherlands, it participated in a working discussion on the implementation of the NIS Directive. At the invitation of a Dutch partner from the National Cyber Security Centre, the Authority participated in one of the most important international conferences of the ONE Conference 2019 in The Hague to present the latest trends and developments in cybersecurity. In June 2019, the Authority participated in a workshop organised by ENISA in Warsaw, Poland. The main theme was the development of national cybersecurity strategies and the exchange of experience on its implementation. Another important activity was the internationally recognised conference held in Katowice, Poland, bringing together experts and speakers from all over the world to discuss and bring new insights on current cybersecurity topics such as 5G network security, artificial intelligence, data protection in cyberspace, smart cities and so on.

EXCHANGE OF FOREIGN INFORMATION

The digitalisation of the 2018 registers of foreign classified information and its online connection with the registers of public authorities allowed to **secure faster and more flexible registration and electronic distribution of classified information.** In 2019, the Authority assisted individual registers of classified information set up by public authorities in the introduction of electronic records of classified information.

9 208 NATO classified information and **3,935 EU classified information** were processed through the Central Registry Office in 2019. The Authority also facilitated the exchange of 145 classified information of foreign power. An overview of the activities of the Central Registry in 2019 and a comparison of data with 2017 and 2018 is given in Table No. 4. The Authority also ran **a registry of NATO classified information ATOMAL**. In 2019, there were no classified documents classified NATO Secret Atomal.

Table No. 4: Exchange of classified documents in 2017-2019

Classification level	2017	2018	2019
NATO Restricted	2 778	2 371	4 870
EU Restricted	4 453	3 773	2 374
Foreign power RESTRICTED	84	60	53
NATO Confidential	1 576	1 851	1 847
EU Confidential	3 34	588	1 131
Foreign power CONFIDENTIAL	13	85	62
NATO Secret	2 367	1 837	2 491
EU Secret	79	208	430
Foreign power SECRET	5	24	14
NATO Top Secret	0	0	0
EU Top Secret	0	0	0
Foreign power TOP SECRET	6	16	16
NATO total	**6 721**	**6 059**	**9 208**
EU total	**4 866**	**4 569**	**3 935**
Foreign power total	**108**	**185**	**145**

3.3 PROTECTION OF CLASSIFIED INFORMATION

In 2019, **there were no incidents and circumstances** that would interfere with the system of ensuring the protection of classified information in the Slovak Republic. In September 2019, the Council of the European Union carried out an inspection of the protection of classified information in the SR. Its official results have not yet been processed. In their preliminary conclusions, the European inspectors gave a positive assessment of the system's design and the operation of its various elements. Overall, they stated a high level of security of classified information in the SR. The North Atlantic Treaty Organisation announced a similar inspection in 2020.

PERSONNEL SECURITY

Carrying out personnel security clearances (PSC) on natural persons is one of the key activities of the Authority. In 2019, the Authority issued **4 268 certificates for familiarisation with classified information**, of which 2 248 were for the Defence Department. An overview of the number of certificates issued between 2017 and 2019 is given in Table No. 5.

Table No. 5: Overview of certificates issued in 2017-2019.

Classification Level	2017	2018	2019
Dôverné (eq. CONFIDENTIAL)	**3 060**	**2 728**	**2 166**
of which Dôverné for Ministry of Defence	1 308	780	730
Tajné (eq. SECRET)	**1 590**	**1 700**	**1 807**
of which Tajné for Ministry of Defence	1 029	1 308	1 351
Prísne Tajné (eq. TOP SECRET)	**377**	**297**	**295**
of which Prísne Tajné for Ministry of Defence	212	154	167
Total	**5 027**	**4 725**	**4 268**

In 2019, the Authority issued **28 decisions**, and natural persons filed **14 appeals** against the decision of the Authority. In either case, the Authority did not decide in the author's office. The Committee of the National Council of the Slovak Republic to review the decisions of the National Security Authority (hereinafter referred to as the 'Committee') decided on 13 appeals, dismissing the appeal in all cases. As at 31 December 2019, one appeal was at the appeal stage.

The decision of the Committee has been brought before the Supreme Court of the Slovak Republic (hereinafter referred to as the Supreme Court), a single action pending before the Supreme Court of the Slovak Republic. In addition, the Supreme Court ruled in 2019 in five cases in which actions were brought in the previous period. In four cases, the Supreme Court dismissed the action. In one case, the Supreme Court closed the proceedings for withdrawing the action. For an overview of the Authority's decisions, appeals and actions brought before the Supreme Court, see Table No. 6.

Table No. 6: Decisions of the Authority, appeals of natural persons against decisions of the Authority and actions in 2017-2019

	2017	2018	2019
Authority's decisions	**28**	**20**	**28**
Appeals	**12**	**10**	**14**
Appeals - in the author's office	0	1	0
Appeals - dismissed by the Committee	14	9	13
Decisions canceled by the Committee	1	1	0
Decisions brought before the Supreme Court	4	1	1

In relation to **classified information forwarded to NATO and the EU**, **4 104 certificates** were issued to the proposed persons in 2019, of which 2 067 NATO certificates and 2 037 EU certificates were issued. Of the total number of NATO certificates, the Authority has issued 22 NATO ATOMAL certificates that authorise access to information on strategic nuclear deterrence of NATO and hand over to a narrow circle of persons.

INDUSTRIAL SECURITY

In the field of industrial security, the Authority carries out Facility Security Clearances (FSC). An entrepreneur's FSC shall aim at obtaining information on businessmen who give reasonable grounds for their national authority to request the creation of classified information or to be forwarded to them. In such a case, it is the duty of the statutory body of the entrepreneur to request the Authority to carry out a security clearance to obtain an FSC certificate.

In 2019, the Authority issued **109 FSC certificates**, 10 of them of the level Vyhradené (eq. RESTRICTED), 76 FSC certificates of the level Dôverné (eq. CONFIDENTIAL), 22 FSC certificates of the level Tajné (eq. SECRET), and one FSC certificate of the level Prísne tajné (eq. TOP SECRET). An overview of the data presented can be found in Table No. 7.

Table No. 7: Overview of FSC certificates issued in 2017-2019

Classification Level	2017	2018	2019
Vyhradené (eq. RESTRICTED)	3	4	10
Dôverné (eq. CONFIDENTIAL)	60	50	76
Tajné (eq. SECRET)	14	16	22
Prísne tajné (eq. TOP SECRET)	0	3	1
Total	**77**	**73**	**109**

In 2019, the Authority issued **23 decisions**. Five undertakings appealed against the decision of the Authority. In two cases, the Authority decided in author's office and two appeals were decided by the Committee which dismissed the appeals of the undertakings. As at 31 December 2019, one appeal was at the appeal stage. There was no lawsuit to the Supreme Court in either case. An overview of the data presented can be found in Table No. 8.

Table No. 8: Decisions of the Authority, appeals of undertakings against decisions of the Authority and actions in 2017-2019

	2017	2018	2019
Authority's decisions	**13**	**24**	**23**
Appeals	**2**	**6**	**5**
Appeals - in authors office	1	3	2
Appeals - dismissed by the Committee	1	3	2
Decisions canceled by the Committee	0	0	0
Lawsuits to the Supreme Court	0	1	0

In relation to NATO and EU classified information, **12 NATO certificates and 12 EU certificates** were issued to entrepreneurs in 2019, which entitle entrepreneurs to acquaint themselves with NATO/EU classified information.

The Authority has **13 contracts for entrepreneur access** to classified information, in 2019 the Authority concluded nine contracts and five additions to the contracts concluded.

SECURITY OF INFORMATION

In 2019, in accordance with the Act on the Protection of classified information, the Authority provided for the receipt of classified information from one entity without a legal successor, the withdrawal of classified information to an unauthorised person and the acts necessary to ensure its protection.

In 2019, the Authority received and sent 3,909 classified documents. A comparison of the number of documents registered in the protocol of classified documents can be found in Table 10.

Table No. 10: Number of classified documents processed at the Authority in 2017-2019

Classification Level	2017	2018	2019
Vyhradené (eq. RESTRICTED)	3 439	3 201	3 655
Dôverné (eq. CONFIDENTIAL)	290	216	247
Tajné (eq. SECRET)	4	4	7
Prísne tajné (eq. TOP SECRET)	0	0	0
Total	**3 733**	**3 421**	**3 909**

PHYSICAL SECURITY AND BUILDING SECURITY

In 2019, the Authority assessed physical security and building security measures to protect classified information of entrepreneurs who were subjected to security clearance. A total of 49 assessments were made and three consents were given to the establishment of a register of classified information.

In 2019, the Authority issued 86 certificates of mechanical barriers and technical security devices.

PROTECTION AGAINST UNDESIRABLE ELECTROMAGNETIC RADIATION

For measures to ensure the protection of classified information from leakage by means of undesirable electromagnetic radiation, the Authority carried out zone measurements of spaces and measurements of technical means and means of encryption of information in a specialised TEMPEST laboratory in 2019. Based on received applications, 876 measurements of technical devices and cryptographic protection of information (CPI) devices and 47 zone measurements of spaces were made, which categorised 241 technical devices and 31 spaces. In 2019, a request was made to carry out measurements of the shielded chambers, on the basis of which six measurements were made of the attenuation of the shielded chamber.

SECURITY OF TECHNICAL PROTECTION DEVICES

In 2019, the Authority issued 67 certificates of technical devices and 25 additions.

Table No. 9: Number of issued certificates in years 2017 – 2019

Classification Level	2017	2018	2019
Vyhradené (eq. RESTRICTED)	5	7	24
Dôverné (eq. CONFIDENTIAL)	28	22	37
Tajné (eq. SECRET)	7	12	6
Prísne tajné (eq. TOP SECRET)	0	1	0
Total	**40**	**42**	**67**
Amendments	16	19	25

ACCREDITATION OF COMMUNICATION AND INFORMATION SYSTEMS

In 2019, the Authority carried out two updates to the accreditation of the BICES communication and information system for the temporary deployment of technical means for handling NATO classified information in accordance with NATO Security Policy C-M(2002)49. In addition, three systems have been accredited for the EU in accordance with Council Decision (2013/488/EU) and one system in line with NATO Security Policy C-M(2002)49.

DIGITALISATION OF AUTHORITY'S SERVICES

In 2019, the Authority implemented a national project to build an **information system for the digitalisation of the Authority's services** in the areas of classified information protection and internal processes of the Authority. The project provided a better and safer environment for dealing with classified information, while reducing the existing restrictions on dealing with classified information. The hardware infrastructure has been upgraded to ensure a higher level of security of the information system, to improve the baselines for monitoring operational environmental indicators, to increase the quality of availability and reliability of individual environments, to create a better working environment with shorter time-response, and to increase the efficiency of work, to improve the quality of individual environments in terms of availability and reliability. The built architecture in the future will enable further development of the system. In 2020, a system certified according to Decree No. 339/2004 Coll. on security of technical means will be built.

TRAINING AND VERIFICATION ACTIVITIES

In 2019, the Authority continued a series of **lectures and trainings focused on individual security areas** in the implementation of the **concept of security awareness building** in the field of classified information. The Authority also conducted the exams of a **security employee**, and in 2019, it issued **276 exam certificates** to the successful graduates.

3.4 CRYPTOGRAPHIC PROTECTION OF INFORMATION

The cryptographic protection system in the Slovak Republic is based on a proven structure of departmental cryptographic bodies and their close cooperation with the Authority, which acts as a central cryptographic authority. In 2019, the Authority provided **management of CPI systems and devices** operated by the Authority and the state administration bodies. It continuously provided the operational requirements of the departments and provided them with related support, especially the production and distribution of national crypto material and consultancy for the maintenance of the systems and devices used.

CRYPTOGRAPHIC PROTECTION OF INFORMATION (CPI) AND TECHNICAL DEVICES

In 2019, the Authority issued **11 certificates of CPI devices** and one supplement to the certificate of CPI device.

In 2019, the technical device for the secure communication of workstations and mobile equipment at the security level of Vyhradené was updated. 32 new user accounts were created in the system. The Authority continued to distribute on an ongoing basis the **technical devices** available for the secure exchange of information between government

institutions under the Confidential and Secret regime. In order to secure the government's connection, these technical devices were provided to 33 registers of government institutions. The technical devices provided replaced earlier CPI devices, which expired the validity of certificates.

ELECTRONIC LOGBOOK

In 2019, the **electronic logbook** of classified information was fully operational. A system adapted by internal resources makes the registration of classified information quicker and more flexible. Prior to the launch, there was training of the staff of the registers of the individual public authorities and the product testing version was also in operation for three months. During 2019, the segment "D", "T" and "TN" were built. These segments cover online communication at a given classification level (DÔVERNÉ, TAJNÉ and TAJNÉ - NATO). These segments were certified and the "D" segment was launched.

3.5 CYBER SECURITY

The increasing dynamics of cyber threats, sophistication and flexibility of attackers in 2019 caused a necessary reaction by implementing appropriate **legislative conditions**, building an **institutional framework**, strengthening **staff capacities**, implementing the latest **technological solutions** and **intensive cooperation** at national and international level.

NATIONAL CYBERSECURITY CENTRE SK-CERT

In accordance with the Action Plan for the Implementation of the Cybersecurity Concept of the SR 2015-2020, the Authority established the **National Cybersecurity Centre SK-CERT (NCKB)** on 1 September 2019. The Centre was created by the transformation of the National Cyber Security Incidents (CSIRT) Unit, operated by the Authority in accordance with the Cyber Security Act since 2018. The NCKB shall provide **services related to the management of security incidents**, their consequences and the subsequent renewal of information systems in cooperation with their owners and operators, as well as the **performance of analytical activities, research, security awareness-raising and cybersecurity education**.

REGISTERS OF OPERATORS AND SERVICE PROVIDERS

In 2019, 142 operators of basic services were included in **the register of basic service operators**, including 37 operators of the basic service as a public administration information system. The number of **digital service providers** increased by two in 2019. In 2018, 100 operators of basic services were included in the register of basic service operators, including 43 operators of the basic service as a public administration information system.

SECURITY INCIDENTS

As part of its preventive activities, the Authority continued to distribute **security alerts** and weekly security newsletters, including address warnings for current security incidents, threats, vulnerability and other relevant information, through SK-CERT. In 2019, **36 255 329 cyber security incidents** were registered, i.e. more than three million incidents per month on average. There was an increase of 14.27 % in recorded incidents compared to 2018. **8 815 incidents were addressed**, 60.2 % more than in 2018. The data are visually shown in Diagrams No. 1 and 2.

Diagram No. 1: Increase in the number of reported incidents in 2019

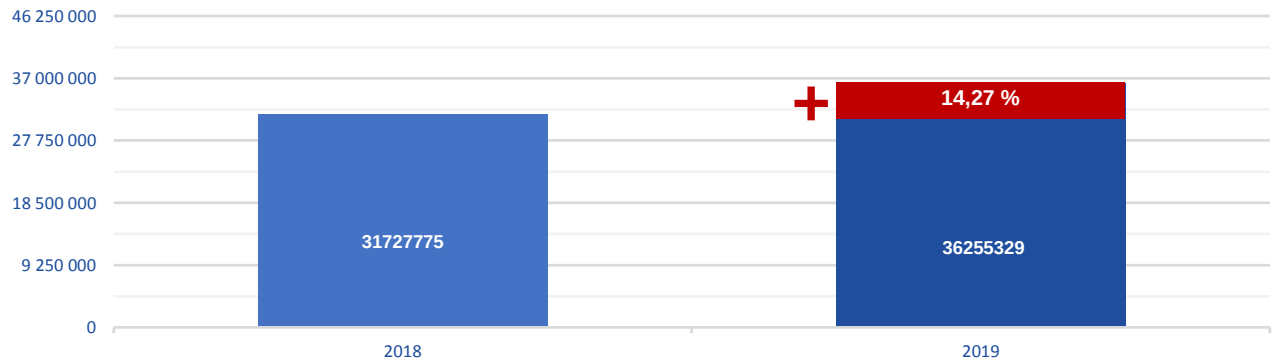


Diagram No. 2: Increase in the number of incidents dealt with in 2019

The most numerous incidents were attacks using **social engineering tools**, especially phishing content. The second largest group of incidents represented attacks in which outdated, non-updated, incorrectly installed or generally **poorly secured systems** were abused. The increase in cybersecurity incidents follows the global trend, affecting all sectors, but also ordinary people.

Diagram No. 3: Overview of registered incidents by type of attack

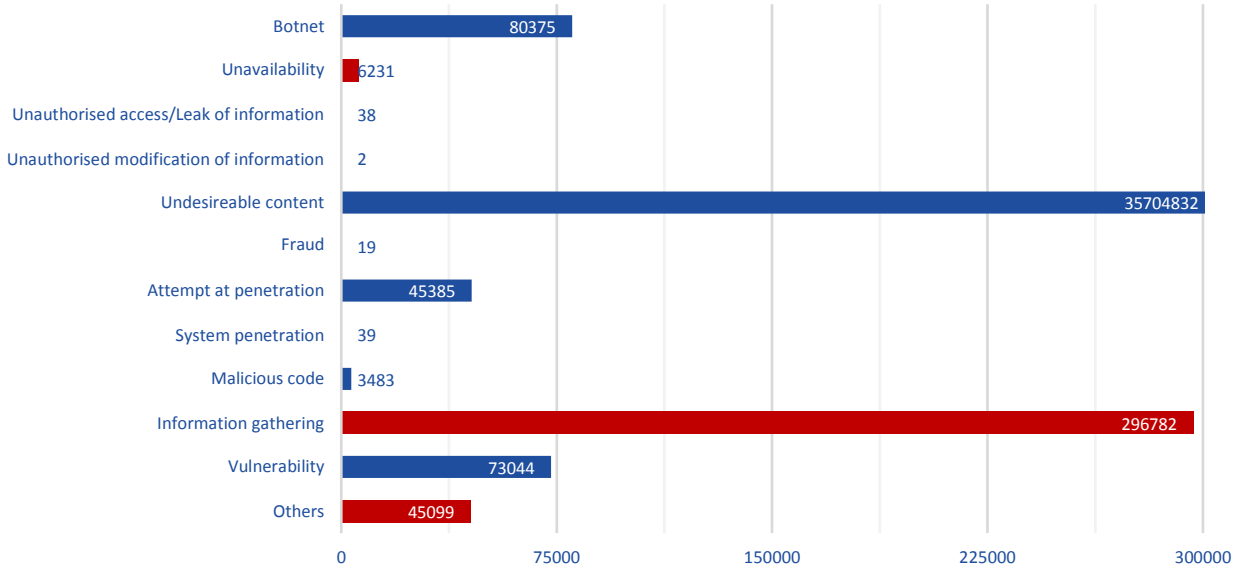
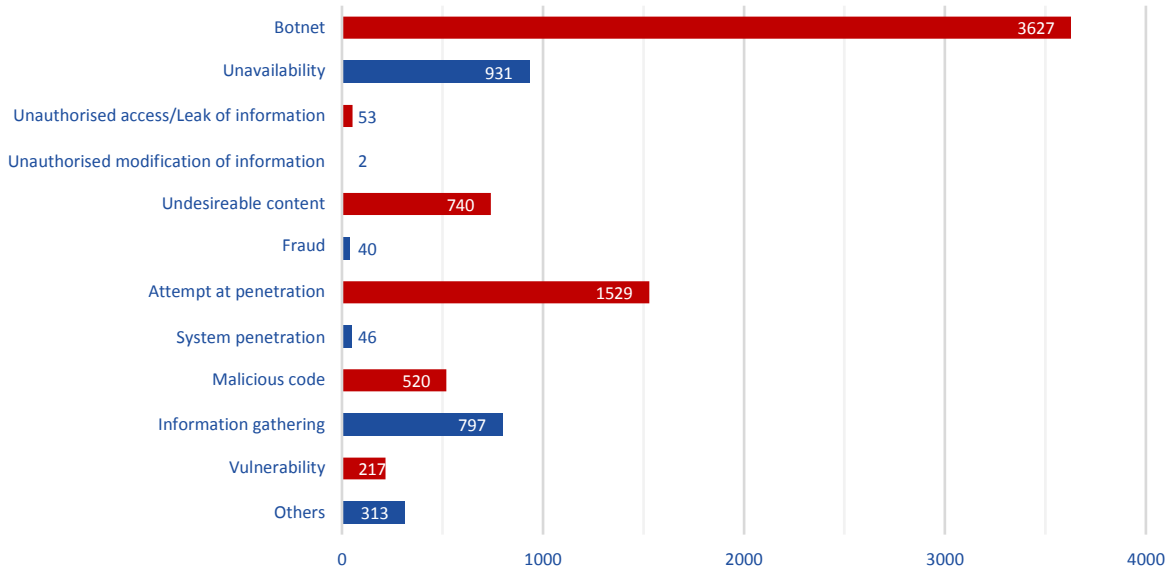


Diagram No. 4: Summary of addressed incidents by type of attack



In October 2019, SK-CERT published a Vulnerability Reporting Guide, which serves as a tool for security researchers, software developers, hardware and equipment manufacturers, as well as the public. The guide provides a detailed procedure and recommended steps to notify newly discovered vulnerabilities as well as a procedure for reporting existing vulnerabilities found in operating systems and services.

TECHNICAL CAPABILITIES BUILDING

In 2019, the Authority continued to build **software and hardware** equipment for SK-CERT to ensure the effective performance of security and operational monitoring, monitoring, detection and evaluation of cyber incidents and threats at national level. Building a **modern infrastructure** is an important aspect for creating optimal high-level cybersecurity conditions not only at SK-CERT's workplace, but by implementing the latest technological trends in **national cyberspace.**

In 2019, the Authority launched **a project to build a National Cybersecurity Incident Management System** in public administration co-financed by the European Regional Development Fund. The main objective of the project is to complete and increase the capacities of the SK-CERT unit infrastructures as well as the completion of specialised centres for complex incident management in terms of legislative competences and legal obligations of CSIRT units. The project activities are currently in the implementation phase with project completion expected to be completed by the end of 2020.

In 2019, **a project** to build **a Center for Cyber Threats Simulation, Research and Teaching and Cybersecurity** was launched. The Authority concluded a partnership contract, with the support of European resources, to carry out eligible activities foreseen for completion in July 2021.

CYBERSECURITY CERTIFICATION

In line with the Authority's intention to further expand its capacity, initial steps were taken in 2019 in the area of cybersecurity certification. In the EU CEF Telecom 2019 programme, the Authority developed **the Cybersecurity Certification Slovakia Project** in autumn 2019 which should help the Authority to carry out accreditation of cybersecurity certification laboratories in the Slovak Republic according to EU legislation and according to the principles and procedures of the globally recognised CCRA certification framework. The project covers the technical areas of certification, accreditation and audit and also envisages mutual support and exchange of best practices and other relevant information with foreign partner organisations. A Communication from the EC on the approval/no approval of project funding is expected in June 2020.

STRENGTHENING STAFF CAPACITIES

The effort to create optimal technical conditions is closely linked to the staffing of SK-CERT. Personnel status of the unit tends to stabilise individual roles of workers, although it is a big challenge to directly occupy positions by **qualified experts** or school graduates. In the cyber area Slovak schools and academics do not prepare students at master's or doctoral level. SK-CERT shall use available capacity models to cover all the services the unit must provide and at the same time to develop the Authority's capabilities in this field in an acceptable manner.

Regular practical training in the form of participation in c**yber-security exercises** such as **LockedShield, SecOPs Europe, Cyber Europe, Cyber Coalition** or **CyberEx** is also an important part of the Authority's continuous enhancement of cyber security incidents. In trainings SK-CERT cooperated closely with the armed forces of the Slovak Republic, the Police Corps of the Slovak Republic, the National Agency for Network and Electronic Services, CSIRT.sk and other state bodies or institutions.

BROADENING COOPERATION

Cybersecurity is mainly about well-functioning cooperation between partners and entities providing sub-tasks in this area. In 2019 there was an **intensification of cooperation at the level of departments**, namely the Office of the Deputy Prime Minister of the Slovak Republic for Investment and Informatisation, the National Agency for Network and Electronic Services, the Slovak Information Service, the Military Intelligence of the Ministry of Defence of the Slovak Republic and the Ministry of Foreign and European Affairs of the Slovak Republic. Intensive communication and cooperation took place with **core service operators, digital service providers and private CSIRTs**. The Authority provided methodological assistance to individual entities in applying the principles of the Cybersecurity Act and consulting on practical problems in implementing legal requirements. In this way, feedback was also obtained, on the basis of which the Authority can provide better services in the future. Closed memoranda on cooperation between the Authority and **professional associations**, in particular the Cyber Security Association, ISACA Slovakia, the Association of Security and Defence Industry and the Civil Association of AFCEA Slovakia, open the scope for implementation of the Authority's intention to connect experts from the public and private spheres and launch an effective and open discussion on common cyber security gaps.

International cooperation on cybersecurity was also intensively developed by the Authority in 2019. For details see Chapter 3.2 International Cooperation.

BUILDING SECURITY AWARENESS

Activities have also been carried out in the field of security awareness dissemination. The Authority has repeatedly recommended compliance with **minimum standards of cyber hygiene**, publishing universally valid advice and guidance on **how to behave safely on the Internet** and how to protect users' personal and sensitive data. In 2019 he also organised a series of national table-top exercises for operators of basic services and selected public administration organisations. They were oriented on the management **decision-making training** of organisations in cyber incidents and their participants were involved in solving fictional cyber incidents with hypothetical events to which they had to react as they would actually happen. They had the opportunity to test the effectiveness of their own procedures and processes, to train the tasks and responsibilities of individual roles and managerial decision-making.

CYBERSECURITY COMPETENCE AND CERTIFICATION CENTRE

In December 2019, the Authority obtained the approval of the Ministry of Finance of the Slovak Republic to establish a contributory organisation, **Competence and Certification Centre for Cyber Security** of the Centre, which started operations on 1 January 2020. The creation of a centre of competence is based on the proposal for a European Regulation to establish a European Centre for Sectoral, Technological and Research Competences in the field of cybersecurity and the creation of a network of national coordination centres. It is also thematically based on the draft regulation establishing the Digital Europe Programme and the Digital Transformation Strategy approved by the Slovak Government in 2019.

The competence of the Centre of Competence (since 1 January 2020) will cover the fulfilment of the tasks of the National Sectoral, Technology and Research Centre in the field of cyber security, namely the tasks of the certification body under the Cyber Security Act, the activities of the authorised person under the Act on the Protection of Classified Information, the provision of services related to the organisation and technical provision of educational activities for the founder. Zone measurements and measurements of unwanted electromagnetic radiation, carrying out expert and expert activities, carrying out scientific, research and development activities in the field of cybersecurity and information-communication technologies and consulting activities in the field of classified information protection, cyber security and trust services, organisation of educational events, courses, trainings and seminars.

3.6 TRUST SERVICES

In accordance with the eIDAS Regulation, Act on trust services and the supervision scheme, the Authority conducts **oversight over qualified trust service providers**. Ex post supervision is performed over the non-qualified providers of trust services, and that only in case the Authority obtains information suggesting that they provide services that do not meet the requirements set out in the eIDAS Regulation.

In 2019, the Auhority issued **one device certificate for creation of qualified signatures and seals**. The Authority received **one request for certification of a security product for qualified electronic signatures**, the proceedings have been stopped due to an approval of certification in another European Union country and its publishing in the List of certified qualified devices for creation of electronic signatures of the European Commission.

TRUSTED LIST

The Authority manages and publishes on its website a trusted list containing **information on qualified trust services providers**, who are under the supervision of the Slovak Republic and information on the provided qualified trust services. During 2019, the Authority published 12 versions of the trusted list.

LIST OF AUTHORISATIONS

The list of authorisations, which is an **information source for qualified trust services providers** for the purpose of issuing mandate certificates, is published by the Authority on its website. In 2019, based on the applications of state authorities and local authorities, 17 new authorisations were added to the list. Its current version has always been supplemented by an archive of the previous versions.

NEW TRUST SERVICES

The Authority received a notification from three **qualified providers about the intention to provide the qualified trust service** of issuing qualified electronic time stamps. The notice had to be submitted by the provisions together with the final report on conformity assessment. In total, **30 qualifying statuses** have been granted for this trust service. In 2019, the Authority assessed and granted the applications of three qualified providers for extension of existing qualified services with the OCSP service (Online Certificate Status Protocol). Concurrently in 2019, four reports on conformity assessments conducted by the conformity assessment body up to 24 months since carrying out the last audit were submitted, which confirmed that qualified trust service providers and qualified trust services that are offered fulfil the requirements set by eIDAS Regulation.

CREATION OF INTERNATIONAL STANDARDS

During the creation of the international technical standards applicable to the implementation of the eIDAS Regulation, a civil servant of the Authority was a project leader for ISO 14533-4 within ISO TC 154. Due to his active participation in the fulfilment of his duties ensuing from this function, the ISO/ DIS 14533-4 standard was issued on 27 August 2019, which included the requirements of the supervision scheme, which the Authority issued as a list of recommended technical procedures of implementation of legislative requirements defined in the eIDAS regulation for qualified services, for which the commission did not issue optional implementing acts.

TRUST INFRASTRUCTURE

The Authority operates the **Root Certification Authority of the Slovak Republic** as part of the trust infrastructure, which issues certificates of public keys and maintains a longterm database of issued qualified certificates with their validity status issued by the providers, to whom the Authority granted the qualified status.

SLOVAK NATIONAL CERTIFICATION AUTHORITY

In year 2019, the Authority by the means of the Slovak National Certification Authority (SNCA) provided free-of-charge **qualified trust services to public authorities**. The SNCA provided the qualified trust service of preparing and verifying the qualified certificates for e-seal, qualified trust service of preparing qualified electronic time stamps and qualified trust service of preparation and verification of qualified certificates for electronic signature - including issuance of mandate certificates.

The number of qualified electronic time stamps issued, and qualified certificates issued for public authorities had a growing tendency in 2019. This trend is expressed in diagrams No. 5 and 6.

Diagram No. 5: Number of time stamps issued in 2019

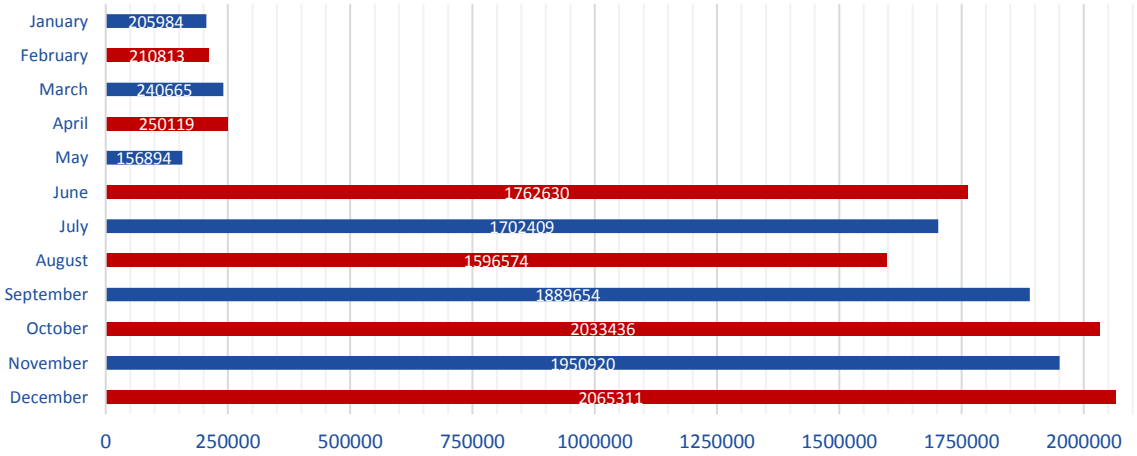
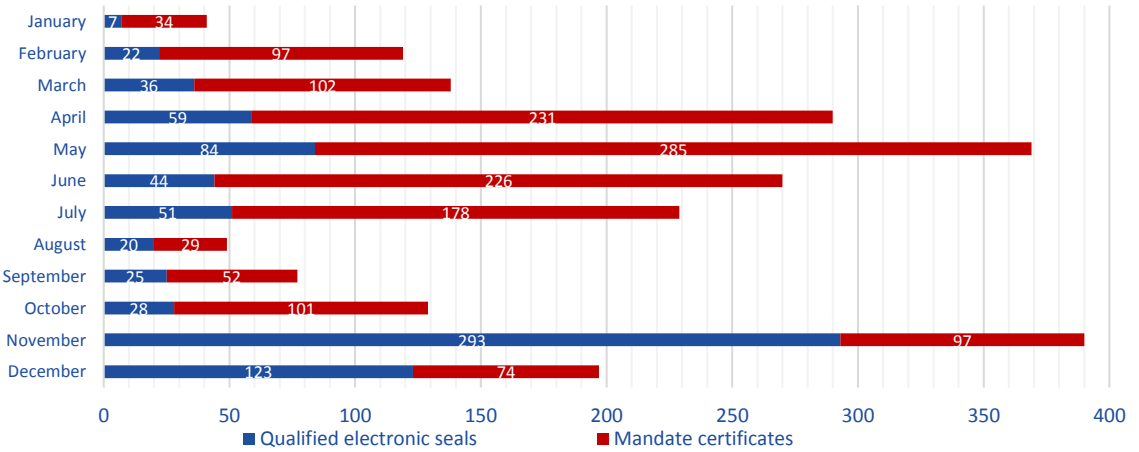


Diagram No. 6: Number of qualified certificates issued in 2019



Providing of SNCA services was in accordance with the Ammendment to the Act on Trust services from 1 August 2019 transferred to the National Agency for Network and Electronic services (NASES). The Authority provided full cooperation and support of maintaining the transferred SNCA services during this period.

4. ECONOMY

In accordance with Act No. 370/2018 Coll. on state budget for year 2019 from 5 December 2010, the binding budget indicators of the state budget for individual chapters for year 2019 were approved, including the NSA.

BREAKDOWN OF BINDING BUDGET INDICATORS

Breakdown of binding budget indicators of Chapter 41- National Security Authority, impact of budgetary measures on budget as of 31 December 2018 and the comparison of the drawing of funds to the revised budget as at 31 December 2018 is presented in Table No. 11.

Table No. 11: Authority budget for year 2019

	Approved breakdown	Adjusted budget	Actual	Fulfilment to the adjusted budget
I. Revenues of the chapter	**22 000,00 €**	**13 955,72 €**	**18 801,17 €**	**134,72%**
A. Mandatory indicator (source 111)	20 000,00 €	11 955,72 €	12 300,72 €	102,89%
Source code 72e	2 000,00 €	2 000,00 €	257,16 €	12,86%
Source code 131I	0,00 €	0,00 €	5 191,74 €	-
Source code 11O1	0,00 €	0,00 €	1 051,55 €	-
B. Funds from the European Union	0,00 €	0,00 €	0,00 €	0,00%
II. Total expenses of the chapter (A + B + C)	**10 120 423,00 €**	**21 316 947,94 €**	**20 908 220,89 €**	**98,08%**
A. Expenses total excluding funds according to article 17 (4) of Act No. 523/2004 Coll. and funds from the EU, out of that	10 118 423,00 €	14 892 418,33 €	14 485 567,52 €	97,27%
A.1 Funds from the state budget - source code 111	10 118 423,00 €	10 695 702,22 €	10 290 845,39 €	96,21%
Source code 131H	0,00 €	2 039 196,97 €	2 037 202,99 €	100,00%
Source code 131I	0,00 €	50 000,00 €	50 000,00 €	100,00%
A.2 Funds for co-financing	0,00 €	2 107 519,14 €	2 107 519,14 €	100,00%
Source code 3AA2		1 133 387,56 €	1 133 387,56 €	100,00%
Source code 3AA3		974 131,58 €	974 131,58 €	100,00%
A.3 Wages, salaries, service income and other personal compensations (610) - source code 111	5 413 246,00 €	5 970 879,00 €	5 748 209,13 €**	96,27%
- out of that the apparatus of the central body	5 413 246,00 €	5 970 879,00 €	5 748 209,13 €**	96,27%
Number of budgetary organisation employees according to the annex to the Resolution of the Government of the Slovak Republic No. 667/2010	241 people	241 people	210 people*	87,14%
- out of that apparatus of the central body	241 people	241 people	210 people*	87,14%
A.4 capital expenses (700) (excluding the funds for co-financing) out of that :	0,00 €	2 181 346,97 €	2 179 340,73 €	99,91%
Source code 111	0,00 €	92 150,00 €	92 137,74 €	99,99%
Source code 131H	0,00 €	2 039 196,97 €	2 037 202,99 €	99,90%
Source code 131I	0,00 €	50 000,00 €	50 000,00 €	100,00%
B. Funds according to Article 17(4) of Act No, 523/2004 Coll., according to which the budgetary organization is entitled to draw this limit up to the amount of budget revenue actually received and is entitled to exceed the expenditure limit in order to achieve higher than budgeted revenue	2 000,00 €	2 000,00 €	123,76 €	6,19%
C. Funds from the European Union	0,00 €	6 422 529,61 €	6 422 529,61 €	100,00%
D. Expenses of the state budget for implementation of the programs of the Government of the Slovak Republic and partial programs of the Government	10 120 423,00 €	21 316 947,94 €	20 908 220,89 €	98,08%
0D9 Information security	9 535 585,00 €	20 888 437,57 €	20 489 181,98 €	98,09%
0EK0U Information technologies financed from the state budget - NSA	584 838,00 €	428 510,37 €	419 038,91 €	97,79%
E. Systematisation of police officers in civil service	216 people	216 people	187 people*	86,57%
Volume of funds for service income in civil service	4 880 555,00 €	5 368 611,00 €	5 290 579,27**	98,55%

* registered number of employees as of 31 December 2019, ** including CyberExchange

The mandatory budget indicators of the authority were complied with in 2019. With management of funds the Authority observed the principles of economy, efficiency and purposefulness while complying with legislative regulations, mainly with the Act No. 523/2004 Coll. on Budgetary Rules of Public Administration, Act No. 357/2015 Coll. on Financial Control

and Audit, Act No. 343/2015 on Public Procurement, Resolutions of the Government of the Slovak Republic and Methodical Instructions and Guidelines of the Ministry of Finance of the Slovak Republic.

BUDGET FOR 2020

The Act No. 468/2019 Coll. on State Budget for year 2020 was approved by the National Council of the Slovak Republic on 3 December 2019. Following the item C.3 of the Resolution of the Government of the Slovak Republic No. 500 from 14 October 2019 to the draft public administration budget for 2020 to 2022 and provision of section 6 (3) Act No. 523/2004 Coll. on Budgetary Rules of Public Administration as amended, the mandatory indicators for 2020 were announced to the Authority.

The expenses of the Authority for 2020 were budgeted in the total sum of EUR 11,381,182.00, out of that EUR 11,096,344.00 within the program 0D9 - Information Security and EUR 284,838.00 within the interdepartmental program 0EK0U - Information technologies financed from the state budget - NSA. The income of the Authority as a binding indicator was budgeted in the sum of EUR 20,000.00, income under the source code 72e was budgeted in the sum of EUR 2,000.

The budgetary funds will be used by the Authority in order to carry out its tasks resulting from the generally binding legal regulations and from the obligations of the Slovak Republic towards the EU and NATO.

5. OVERSIGHT AND AUDIT

The oversight and audit activities are often perceived by the audited entities as an unpleasant and repressive activity, although it also has a preventive and educational meaning. It also provides precious knowledge and feedback on the condition of compliance with the generally binding legal regulations and contributes to significant improvement of the legislative activity of the Authority.

The Authority continued the oversight activities of state authorities and entrepreneurs in 2019. In **the field of protection of classified information**, it carried out three **planned and one extraordinary check**, all of them in state authorities. The inspection teams focused mainly on the complexity of adopted security measures and their coordination throughout each field of security. Deficiencies were identified in three entities. A total of fifteen findings were found, five of which were in the area of security of information, four in the area of physical and facility security, four in security of technical devices and one deficiency in both industrial security and cryptographic protection of information.

Table No. 12: Oversight activities of the Authority for 2019

Entity	Number of inspections		Area	
	Planned	Extraordinary	Classified information	Trust services
State authority	3	1	4	0
Entrepreneur	0	0	0	0

The inspection activity was carried out comprehensively and focused on all areas of security and their mutual interconnection in the system of ensuring the protection of classified information. Overall it is possible to state that in comparison with the previous period**,** the **number of inspection findings have increased**.

METHODOLOGICAL ACTIVITY

The Authority was repeatedly approached by state authorities throughout 2019, by state authorities, entrepreneurs as well as individuals, with requests for **methodological guidelines** for all areas that fall under its responsibility. The questions most frequently concerned the area of protection of classified information, followed by the field of cybersecurity and trust services. The overview is included in Table No. 13.

Table No. 13: Overview of the methodological activity of the Authority in 2019

Area	Classified information *						Cybersecurity	Trust services
Number	PS	SI	InS	PhS	STD	CSO		
Partial	22	13	15	9	7	24	23	9
By area	90						23	9
Total	**122**							

** PS - personnel security, SI - security of information, InS - industrial security, PhS - physical security, STD - security of technical devices, CSO - cross-sectional opinions*

INTERNAL OVERSIGHT AND AUDIT

The internal audit body in 2019 performed **nine internal inspections**. The four concerned material accomplishment of tasks from the government resolutions. Other inspections were mainly focused on protection of classified information in the field of security of technical devices, condition of fire protection, OSH status checks, and inspections of service time of authority officers and on site financial control. Apart from a minor incident of small impact, no severe infraction of generally binding legal regulations was identified during the inspections.

The Internal audit unit carried out **four internal audits** in 2019. These were focused on verification and evaluation of registries and claim recoveries, the process of internal procurement, spending of public resources on foreign business trips and the financial impact of officer and employee sick leave on the budget and the separate account of the Authority. The executed audits identified one liable person defect of low impact, which was unsystematic and financially incalculable.

COMPLAINTS AND PETITIONS

There were no complaints or petitions delivered to the Authority in 2019.

6. CONCLUSIONS AND PRIORITIES FOR 2020

Year 2019 was rich in events, which had a direct impact on the status, operation and perception of the authority. The Authority's activities included a wide range of tasks, many of which will be developed or completed in the upcoming years.

No extraordinary circumstances occurred in 2019 which would disrupt the system of classified information protection in the Slovak Republic. An inspection was carried out by the Council of the EU in September, its unofficial preliminary conclusions confirmed a **high level of protection of classified information**, the correctness of the system setup and effects of its individual elements. There were also no substantial problems which would restrict functionality of the network of classified communication of constitutional actors and other government officials. The security of the **government connection** was not endangered and it was carried out via certified technical devices and certified crypto devices.

The Authority continued to introduce **viable legislative conditions**, which were a necessary reaction to development trends and problems which appeared in applied practice. The development of the **institutional framework** continued, along with strengthening of **personnel capacities** of the Authority and implementation **of improved solutions and best practices**.

The personnel status of the Authority aims toward stabilisation of individual roles, although in case of some positions, it is a tremendous challenge to fill them with **qualified professionals**.

The **Authority cooperated with the security authorities of EU and NATO in 2019** in all fields of its responsibility. It performed active steps toward **support of regional cooperation and bilateral partnerships** allowing the exchange of experience, formulation of common standpoints and coordination of procedures in asserting common interests. The Authority provided for the **international exchange of classified information**. The digitalisation of the registers of foreign classified information and its online connection with the registers of public authorities allowed secure and **faster and more flexible registration and digital distribution** of classified information.

In the field of cybersecurity, the Authority responded to the rising intensity and dynamic form of threats in 2019. Cyber attacks were distinguished by use of **new or innovative techniques and application of new attack vectors**. Aside from state actors and state sponsored groups which conducted espionage activities, tried to manipulate the public opinion or manipulate the results of democratic processes, there are also individuals operating in cyberspace for whom cyber attacks are a personal challenge, but also a source of income.

The Authority established the **National Cyber Security Center SK-CERT (NCKB)** on 1.st September 2019, which secures **services connected with managing security incidents**, removing their consequences and subsequent renewal of activity of information systems in cooperation with their owners and operators, but also the **performance of analytical activities, research, raising security awareness and education**.

For the sake of sustainability of task performance of the Authority and in the perspective of Authority progress in the upcoming period, the **Development Strategy of the National Security Authority for years 2019-2026** was developed. The material summarizes the scheme of development priorities of the Authority and defines strategic goals in the field of strengthening the identity of the Authority, establishing personnel capacities, increasing the expertise of performed tasks, optimalisation of internal processes and development of external relationships. The goals are based on the idea of desired state in the future and are broken down into specific activities which allow their execution by implementing specific measures into practice.

In accordance with the development intentions of the Authority for 2019, the model of **program and project management of teams** was implemented, which secure the **fulfillment of cross–sectional and interdepartmental tasks**. The teams deal mostly with preparation and execution of projects co-financed by European funds. One of the most important prijects, which execution is underway, or in in the process of preparation is the **National System of Incident Management** of cyber security in government, the project of establishing the **Center of Simulation, Research and Education** of cyber threats and cyber security, the project of **Certification of Cyber Security**, the project of **Digitalisation of Authority Services in the Field of Classified Information**, and the project of Implementation and Support of Quality Management in government. Each of the projects has high ambitions to contribute to the effectiveness of applied processes, prepare qualified professionals and secure modern technical equipment. The individual projects will be finalised throughout 2020 and 2021.

The Authority processed its own **Anti-corruption program** in 2019 and adopted the **Ethical codex**. Both these documents are tools of positive motivation of Authority personnel, strengthening the sense that they work in an ethical environment with clear rules applicable to everyone. The Authority has the ambition to implement the system of managing corruption risks in 2020 according to STN ISO 37001 Systems of management against corruption and in parallel with the internal system of reporting antisocial activity to create, maintain, investigate and improve the system of management against corruption.

The activity of the National Security Authority dates back to 2001. It holds the role of central authority for the field of protection of classified information, crypto service, cyber security and trust services.

The National Security Authority, as a part of the security apparatus of the Slovak Republic carries out security clearence checks of individuals and entrepreneurs, provides secure government connection, is the oversight authority for trust services and fulfills the role of the national unit for resolving cyber security incidents.

In relation to foreign countries, the National Security Authority is the contact point and national authority for areas within its responsibility.

From 2019 the National Security Authority within its organisational structure operates the National Cyber Security Center SK-CERT.

National Security Authority
Budatínska 30, 851 06
Bratislava

podatelna@nbu.gov.sk
media@nbu.gov.sk
www.nbu.gov.sk