NATIONAL SECURITY AUTHORITY

2017 ANNUAL REPORT

Bratislava, March 2018

LIST OF CONTENTS

1. ORGANISATION IDENTIFICATION

NAME	National Security Authority
REGISTERED OFFICE	Budatínska 30, 851 06 Bratislava
TYPE	central government authority
STATUTORY BODY	Jozef Magala, 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 "authority") is responsible for the creation and implementation of state policy for the area of protecting classified information, cryptographic service, cybersecurity and trust services.

In the field of **protection of classified information**, the authority performs security clearance of natural persons and entrepreneurs, collects information on the candidates for appointment as judges and provides evaluation to the Judicial Council of the Slovak Republic, which forms a base for its decision on meeting the preconditions for magistracy capacity, keeps the register related to the protection of classified information, performs certification of technical devices, mechanical barrier devices and technical protection devices, provides inspection of classified information in state and self-governing authorities and legal persons. In international exchange of classified information, it serves as a central register of classified information in the Slovak Republic and participates in the protection of foreign classified information (information of other countries, NATO and the EU).

In the field of **cryptographic protection of information** (hereinafter referred to as "CPI"), the authority serves as a central cryptographic authority, ensures secured government and foreign connection, performs certification of CPI means, provides safety inspection of CPI, issued CPI security standards and coordinates research and development of CPI means. It is a guarantor and national authority in international cooperation in the field of CPI and serves as the National Distribution Authority, which is the input and contact point in the Slovak Republic upon the exchanges and distribution of cryptographic material and encryption facilities.

In the field of **trust services**, the authority is a supervisory authority in the Slovak Republic. Its tasks involve certification of facilities for the 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 key certification authority in the Slovak Republic issuing certificates of public keys to qualified providers of trust services.

In the field of **cybersecurity**, the authority performs tasks of conceptual, legislative and methodical character, which involve creation, coordination and implementation of state policy in the area of cybersecurity. It also takes into consideration the international aspects of cybersecurity and represents the Slovak Republic in international organisations, mainly in NATO and the EU.

KEY LEGAL REGULATIONS

In the accomplishment of the set tasks, the authority is governed by the Constitutions 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.

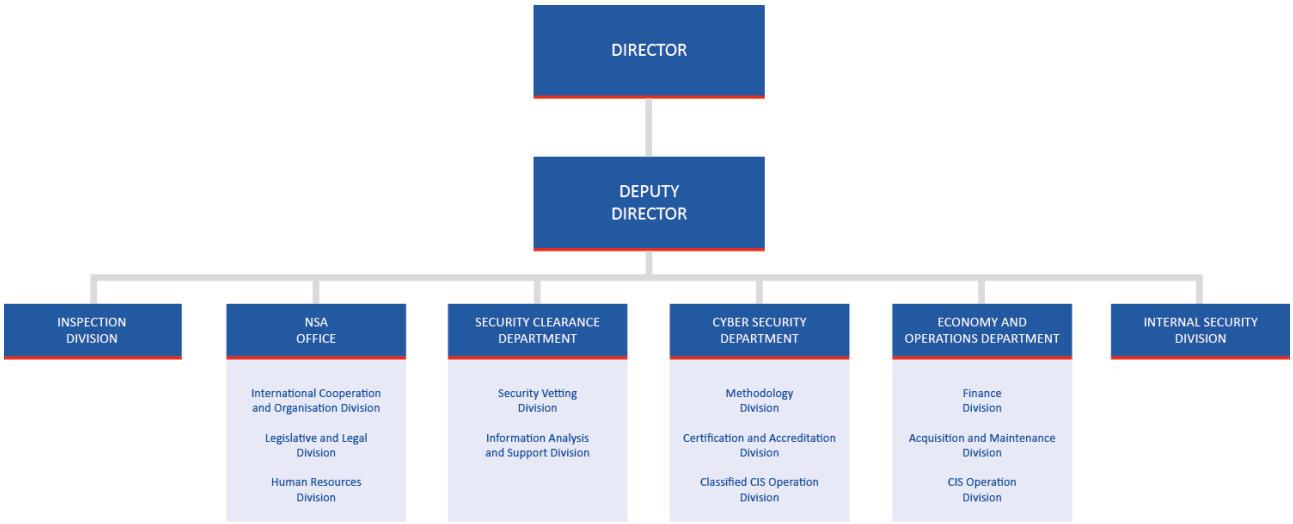
The base of the authority activities in the field of protection of classified information and cryptographic protection of information is formed by the **Act No. 215/2004 Coll. on protection of classified information** and on amendments and supplements of certain acts, as amended (hereinafter referred to as "Act on Protection of Classified Information"). The field of trust services is regulated by the 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 (hereinafter referred to as "eIDAS Regulation"), **Act No. 272/2016 Coll. on trust services** for electronic transactions on the internal market and on amendments and supplements of certain acts (Act on Trust Services) and **Act No. 69/2018 Coll. on cybersecurity** (came into force on 1 April 2018).

LEADERSHIP OF THE AUTHORITY

The authority is headed by the **Director**, who is responsible for the activity of the authority, 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 public servants. He covers the inter-ministerial cooperation of the authority and is a permanently invited 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 reserved scope represented by the **Deputy Director of the Authority**, who is also responsible for coordination of the activities of units.

ORGANISATIONAL STRUCTURE

From the organisational point of view, the authority is divided into **departments and directly managed divisions.** Departments are further divided into divisions. The internal organisational structure in 2017 is represented by the following scheme.



UNITS OF THE AUTHORITY

The **NSA Office** coordinated the activity of the authority units, performed basic administrative and organisational activities related to the management and activities of the authority, arranged legislative and legal matters of the authority, implemented the personnel and wage policy of the authority, coordinated international cooperation, built and developed external relationships and cooperation, and ensured communication to the public.

The **Security Clearance Department** performed security clearances of natural persons and legal persons (entrepreneurs), collected documents for the decision of the Judicial Council of the Slovak Republic on the competence of candidates for appointment as judges and issued certificates for access to classified information of the North Atlantic Treaty Organization (hereinafter referred to as "NATO") and of the European Union (hereinafter referred to as "EU").

The **Cyber Security Department** performed accreditation and certification in the field of protection of classified information for personal security, administrative security, physical security, and building security, security of technical devices and industrial security, in the field of cryptographic protection of information, in the field of cybersecurity and in the field of trust services. It served as a central coordination and technical centre in the field of cybersecurity and operated the national unit of CSIRT (SK-CERT). It further coordinated and performed the tasks of public regulated service provided by the global satellite navigation system established within the Galileo Program and served as the National Security Analytics Centre.

The **Economy and Operations Department** provided for the financial management of the authority, coordination in the process of management of funds, including accounting and reporting, management and maintenance of the authority property, public procurement for the needs of the authority. It further implemented and maintained the course and operation of information and communication systems of the authority.

The **Inspection Division** performed inspections of the protection of classified information and inspection of adherence to the terms and conditions of providing trust services in state authorities, municipalities, upper territorial units and other legal persons. It also performed examination of security employees.

The **Internal Security Division** ensured internal security of the authority and provided for physical and technical protection of the premises of the authority. It also performed internal inspection and financial inspection, internal audit and also handled complaints and petitions.

2. HUMAN RESOURCES

Officers work at the authority pursuant to the 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 public servants in employment relationship pursuant to the Act No. 552/2003 Coll. on performance of work in public interest.

The total number of authority staff was relatively stable for the last three years, while it increased negligibly from 214 to 217 (+ 1.38%). The ratio between the number of officers and public servants did not change fundamentally either; the rate of a slightly higher number of women over men also remained. The almost double amount of officers included in preparatory civil service is on one side related to the natural staff change but also with the performed recruitment of experts, who will participate in the building of capabilities of the authority in the field of cybersecurity. The data representing the above evaluations (currently as of 31 December of the respective calendar year) are recorded in detail in Table No. 1.

Table No. 1: Number of officers and public servants in 2015 - 2017

	2015	2016	2017
Officers	**193 (90.19%)**	**197 (91.20%)**	**197 (90.78%)**
in preparatory civil service	11 (5.70%)	17 (8.63%)	19 (9.64%)
in permanent civil service	180 (93.26%)	176 (89.34%)	177 (89.85%)
in temporary civil service	2 (1.04%)	4 (2.03%)	1 (0.51%)
Public servants	**21 (9.81%)**	**19 (8.80%)**	**20 (9.22%)**
Total	**214** (115 women and 99 men)	**216** (117 women and 99 men)	**217** (115 women and 102 men)

In 2015, we managed to put an end to the weakening of the most represented age group of 35 to 49 years. Although in 2017 the continuous growth of this group slightly slowed down (54.83% compared to 55.56% in 2016), its representation did not fall under the level of year 2014 (51.77%) or year 2015 (52.80%). This group includes experiences experts with several years of practice in the most productive age. All the data on the age structure of the authority is included in Table No. 2.

Table No. 2: Age of officers and public servants in 2015 - 2017

	2015		2016		2017	
	Officers	Public servants	Officers	Public servants	Officers	Public servants
	193 (100%)	**21** (100%)	**197** (100%)	**19** (100%)	**197** (100%)	**20** (100%)
Younger than 34 years	**41** (21.24%)	**1** (4.76%)	**39** (19.80%)	**0** (0.00%)	**39** (19.80%)	**1** (5.00%)
35 to 49 years	**109** (56.48%)	**4** (19.05%)	**117** (59.39%)	**3** (15.79%)	**117** (59.39%)	**2** (10.00%)
50 to 59 years	**36** (18.65%)	**8** (38.10%)	**33** (16.75%)	**9** (47.37%)	**32** (16.24%)	**10** (50.00%)
Older than 60 years	**7** (3.63%)	**8** (38.10%)	**8** (4.06%)	**7** (36.84%)	**9** (4.57%)	**7** (35.00%)

The authority enables its officers and public servants to maintain their professional expertise, gain new skills and deepen their qualification at professional courses, seminars and trainings at home and abroad as well. If necessary, it also ensures increasing of their qualification at universities. For newly hired officers, every year it organises, in cooperation with the Academy of the Police Force in Bratislava, specialised police education, which is a condition for inclusion of the newly hired officers in permanent civil service. The data on the education structure of officers and public servants of the authority is included in Table No. 3.

Table No. 3: Education of officers and public servants of the authority in 2015 - 2017

	2015		2016		2017	
	Officers	Public servants	Officers	Officers	Public	Officers
	193 (100%)	**21** (100%)	**197** (100%)	**19** (100%)	**197** (100%)	**20** (100%)
University - Level III	**6** (3.11%)	**0** (0.00%)	**8** (4.06%)	**0** (0.00%)	**9** (4.57%)	**0** (0.00%)
University - Level II	**155** (80.31%)	**6** (28.57%)	**155** (78.68%)	**6** (31.58%)	**154** (78.17%)	**6** (30.00%)
University - Level I	**4** (2.07%)	**0** (0.00%)	**2** (1.02%)	**0** (0.00%)	**4** (2.03%)	**0** (0.00%)
Full secondary	**28** (14.51%)	**13** (61.90%)	**32** (16.24%)	**11** (57.89%)	**30** (15.23%)	**12** (60.00%)
Basic	**0** (0.00%)	**2** (9.52%)	**0** (0.00%)	**2** (10.53%)	**0** (0.00%)	**2** (10.00%)

3. FIELDS OF ACTIVITY

Upon the fulfilment of tasks, the authority takes into consideration the legal framework determining its activities. Several executive, as well as legislative, administrative and other support activities are related to the accomplishment of determined tasks.

3.1 LEGISLATION

GENERALLY BINDING LEGAL REGULATIONS

In 2017, works on the preparation of the new **Act on Protection of classified Information** continued, whose purpose was to determine the optimum principles and minimum standards for creation of a secure environment for classified information. The authority tried to prepare the bill of act with maximum precision so that with respect to its sufficient predictability it met the requirements for the quality of the act and ensured necessary protection of the security interests of the Slovak Republic, as well as of the interests of NATO and the EU.

In 2017, some transitional periods were finished, which were fulfilled and coordinated by the authority based on the **Act on Trust Services and the eIDAS Regulation.** By termination of the transitional periods, which enabled to temporarily accept national solutions, the procedures in the field of trust services were united in the EU. Hereby uniform granting of qualified statute to trust service and **uniform provision of qualified trust service on the entire digital market of the EU** was ensured. Qualified trust services provided in one member state must be equally recognised also in another member stated based on the constitutive character of data included in the national trust list, which is maintained in the list published by the Commission of the EU.

In 2017, the authority completed working on the preparation of the bill of **Act on cybersecurity** and was submitted to the legislative process. After completion of the inter-ministerial commenting process, within the framework of which several comments of stakeholders were incorporated in the bill of act, the act was adopted by the Government of the Slovak Republic on 8 November 2017. **The National Council of the Slovak Republic adopted the Act No. 69/2018 Coll. on cybersecurity** on 30 January 2018 and it came into force on 1 April 2018.

The purpose of the law is to **create a functional legislative framework** enabling efficient implementation of key measures important for the security of the national cyberspace, and at the same time transposes into the Slovak law the priorities and requirements of the Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (hereinafter referred to as "NIS Directive"). The law comprehensively covers the issue of **solving and ensuring security in cyberspace** in the Slovak Republic. It concentrates the reporting of cybersecurity incidents in one single information and communication point and standardises the security requirements nationwide in compliance with the international standards in the field of cybersecurity, and hereby contributes to harmonisation of this issue in the European environment.

The act regulates **organisation and competence of the public authorities** in the field of cybersecurity, assumes the adoption of a national strategy of cybersecurity, introduces a uniform information system of cybersecurity, defines the position and determines the obligations of basic service operators and providers of digital services, adjusts the organisation and competence of units for solving cyber incidents (CSIRT), creates a system of ensuring cybersecurity and defines the minimum requirements for its assurance. Through its provisions, it supports research and education, including the increase of security awareness in the field of cybersecurity and sets the inspection and audit mechanisms in this field.

The authority, in compliance with the requirements of the valid legislation, elaborated in 2017 a preliminary opinion on the EU draft legislative act - Cybersecurity Act (Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification). The second preliminary opinion concerned the draft non-legislative act - Council Decision on the position to be adopted, on behalf of the European Union, within the EEA Joint Committee concerning an amendment to Annex XI **(Electronic communication, audio-visual services and information society)** to the EEA Agreement. Both position papers, after approval in the Departmental Coordination Group for European Affairs, were sent to the Committee of the National Council of the European Union for European Affairs.

INTERNAL REGULATIONS

In 2017, the authority issued **12 regulations** of the authority director and **27 orders** of the authority director. The new regulations were issued for the purpose of implementation of the generally binding legal regulations (e.g. the new registry regulations, public procurement, financial management and financial inspection), with the aim to make the internal processes more efficient (e.g. the new establishment plan, clearance activities and internal inspection, use of telecommunication services, preparation of officers for civil service). The orders of the authority director served for **determination of the holders of certain tasks** in training, interdepartmental cooperation and inventory management.

ADMINISTRATIVE AND INFRINGEMENT PROCEDURES

In 2017, the authority received **one report on unauthorised handling** of classified documents and seven motions for initiation of administrative procedure or infringement procedure. The authority, as **administrative authority** in the field of classified information, acted in two cases, while it imposed fines in the sum of EUR 2,200 within the administrative procedures. During the verification of the motions, no reasons were identified for the initiation of an administrative procedure and acts in the matter of offences.

EXPERT ACTIVITY

The authority is an **expert organisation** registered in the list of experts, interpreters and translators maintained by the Ministry of Justice of the Slovak Republic in the field 520000 - protection of classified information. In 2017, the respective authorities did not apply to the authority for expert assessment.

3.2 INTERNATIONAL RELATIONS

In 2017, the authority cooperated with the security authorities of the EU and NATO in the field of cybersecurity and participated in the protection of classified information of these institutions. It also developed active steps leading to extension of the number of bilateral partnerships enabling the exchange of experience, coordination of procedures and formulation of joint statements in the field of the EU and NATO. The **central register** work unit intermediated **international exchange of classified information** and ensured their protection.

OPERATION IN THE BODIES OF THE EUROPEAN UNION

The officers of the authority regularly participated in the sessions of the **Security Committee of the Council of the EU (Council Security Committee = CSC)**, which fulfils advisory role of the General Secretariat of the Council in the preparation of security policies for the **protection of classified information** of the EU (EUCI). The main focus of the agenda related to the protection of EUCI in 2017 was the revision and creation of security policies in this field. The authority was also represented in the **Safety Certification Council** of the Council Security Committee (CSC (SAB)) and in the **sub-committee for Information Security** of the Council Security Committee (CSC (IA)). Through their experts, in the field of protection from undesirable electromagnetic radiation, the authority participated in the session of the implementation task force for TEMPEST (ITTF).

In the sessions of the **European Commission**, the authority participated in the sessions of the Group of Experts of the European Commission for Security Policy (ComSEG) and Expert Security Committee on Global Navigation Satellite System (GNSS SB), as well as the sessions of SAB - Safety Accreditation Board of the European GNSS Agency (GSA) in the building of the Galileo satellite system.

The **European External Action Service (EEAS)** has a Security Committee of EEAS and a sub-committee for accreditation established, whose sessions on behalf of the Slovak Republic were participated by the officers of the authority.

In the field of **cyber security** in the EU, in 2017 the most loudly resonating topic was the **transposition of the NIS Directive** to the national legislations. The directive created an integrated concept of ensuring cyber security in the member states and defined the necessary security requirements for the competent authorities. Through the authority, the Slovak Republic intensively participated in deepening of the mutual strategic and operational cooperation in the field of the EU and in exchange of experience and implementation procedures related to the NIS Directive, and that mainly with active participation in the sessions of the **Group for Cooperation, Network of Units for Solving Computer Incidents (CSIRT Network), expert task force** and **comitology committee** of the European Commission for the NIS Directive.

By the virtue of the authority, the Slovak Republic intensively cooperated with the **European Union Agency for Network and Information Security (ENISA),** which from its position as the centre for cybersecurity in the EU, helps the member states to be better equipped and prepared for the prevention, revelation and solving of cybersecurity problems. The cooperation involved solving and coordination of reactions to global cyber incidents and concerned the share in the performance of activities of the ENISA agency, commenting on the decisions and representation in the **Management Board of the ENISA agency.**

The officers of the authority actively operated also in the framework of the **Horizontal Working Group for Cyber Matters (HWP)**, where the so-called **Cyber Diplomatic Toolbox** (Council conclusions on common EU diplomatic response to malicious cyber activities) and related implementation guidelines were elaborated. The documents were then approved by the Council on Foreign Relations. The toolbox was introduced into practice by EEAS in December 2017.

HWP elaborated and the General Affairs Council approved (November 2017) also the Joint Communication to the European Parliament, the Council (**Resilience, Deterrence and Defence:** Building strong cybersecurity for the EU) and the related **Action Plan to implement** the Council's Conclusions.

In September 2017, the European Commission introduced the so-called **cyber package** including initiatives in the field of cybersecurity. It contains evaluation of the ENISA agency and proposal for its new mandate, evaluation of the

Cybersecurity Strategy of the EU from 2013 and European Commission's recommendation for a coordinated response to cyber incidents and large-scale crisis (Blueprint). The cyber package also includes the draft Cybersecurity Act, which proposes re-assessment of the mandate of ENISA agency and change of the European certification framework.

In 2016, the authority was one of the founding members of the **European Cyber Security Organisation (ECSO)**, where it also actively operated during the whole year of 2017. Within the organisational structure of ECSO, the authority is a member of the National Public Authorities Representatives Committee (NAPAC) and an observer in the management board. ECSO created six working groups (Working Groups, WG), and through its representatives, the authority participated in the work of three groups (WG1: certification, standardisation, WG5: education, building security awareness and trainings in the field of cybersecurity, WG6: strategic research and innovation agenda). Aimed at the increase of the awareness of ECSO the Slovak professionals, in October 2017, the authority organised a workshop focused on presentation of the ECSO activities in Bratislava within the projects of public and private partnership in the area of cybersecurity.

OPERATION IN THE BODIES OF THE NORTH ATLANTIC TREATY ORGANIZATION

The authority actively participated in the regular **Spring and Summer sessions of the NATO Security Committee (SC)** at the level of directors of security authorities of the member states. The committee deals with the issues related to security policy of the alliance and is an advisory body to the **North Atlantic Council (NAC).** In 2018, the meeting of the NATO Security Committee will take place in Slovakia.

In the **Security Policy Committee**, the representatives of the authority participated in an extensive revision of the standard **C-M(2002)49** (security policy of NATO) and its additional directive in the field of personal, administrative, physical and building security. In 2017, the Committee also revised the standard **C-M(68)41** regulating the protection of information of the ATOMAL classification level and the standard **C-M(2002)50** (anti-terrorism safeguards of NATO bodies) and dealt with security processes ensuring the protection of classified information while sharing information with non-member countries/entities.

In the context of development in the security environment and after recognition of cyber space as an operational domain of NATO (Warsaw Summit 2016), the issue of cybersecurity has gained ground more significantly in the interest of NATO bodies. The representative of the authority acting at the Permanent delegation of the Slovak Republic to NATO in Brussels (hereinafter referred to as "PD SR to NATO") regularly participated in the sessions of the Cyber Defence Committee (CDC) of NATO and participated in the preparation of strategic NATO documents.

The authority also operated within the platform of MISP (Malware Information Sharing Platform), which enables informal exchange of information of cyber threats among the 24 member countries.

The authority as a national point of contact, participated in the preparation, course and evaluation of the cyber defence exercise of **NATO Cyber Coalition 17,** focused on verification of the process, technical and communication skills of the participants.

Active operation of the authority within the NATO also reflected in its participation in the **international project of cybersecurity in education** focused on the creation of education programs and activities to be covered by the Lisbon **NCI Academy** (NATO Communication and Information Academy).

Within the project of **building a new NATO seat**, the authority dealt with the last details related to the systems of physical and building security and protection using electronic security devices and prepared for the moving of delegation to take place in 2018. At the same time, it closely collaborated with the ministries of foreign affairs, defence, interior, the Slovak Information Service and the Military Intelligence.

In 2017, the officers of the authority operated in the NATO Security Committee in the format for **security of information and communication systems** and the NATO Sub-committee for **information security and cyber protection.** They participated in the sessions of working groups focused on the field of cryptographic protection of information, design of communication protocols security policies, mainly Secure Communications Interoperability Protocol (SCIP), International Interoperability Control Working Group (IICWG), NATO PKI Management Authority (NPMA), NATO PKI Advisory Group (NPAG), Crypto CaT, Spec CaT, NATO – BICES – BSWG a NATO – BICES – BSAB.

Aimed at adapting the security procedures in a constantly developing security environment and taking into consideration the changing trends in the defence industry and in the field of international industrial security, the authority operates in the multinational **working group MISWG** (Multinational Industrial Security Working Group). It is made up by the NATO members states (except for Iceland) and states, which are not NATO members (Austria, Finland, Sweden, Switzerland, Israel, New Zealand, and Australia) a creates joint measures and procedures in the protection of classified information related to international defence programs and matters of industrial security in an international context.

In September 2017, with presence of the representative of the authority, the 32nd plenary session of MISWG took place in Gent, Belgium, which provided a platform for exchange and sharing of experience of the representatives of partner

security authorities with performance of security clearance screenings of entrepreneurs, evaluation of security risks and their elimination.

ORGANISATION FOR SECURITY AND COOPERATION IN EUROPE (OSCE)

The **Organisation for Security and Cooperation in Europe** (OSCE) and its informal working group for cyber issues was a new challenge for the operation of the authority. As of July 2017, the authority is the official and **single point of contact for cybersecurity** for the Slovak Republic and plays an active role in fulfilment of the set goals of this group. Year 2018 will be utilised by the authority to prepare the activities related to the presidency of the Slovak Republic in OSCE in 2019. One of the major topics of the presidency will be cybersecurity.

REGIONAL COLLABORATION

In 2017, the **intensity and quality of regional collaboration significantly grew** in the field of cybersecurity. The authority represents the Slovak Republic in the **Central European Cyber Security Platform** (CECSP) made up by the Visegrad Group countries (Czech Republic, Hungary, Poland, Slovakia) and Austria.

Within the presidency of the Slovak Republic in CECSP in 2017, in May the authority organised in Bratislava a session of the platform at the strategic decision-making level. During this session, they addressed the current challenges connected with the **transposition of the NIS Directive** into the national legislations. The second session was organised in November and took place at the operational level. The main topic was strengthening of collaboration involving mainly exchange of experience, sharing information, organisation of joint exercises and formulation of coordinated opinion concerning the cybersecurity agenda within the field of the EU and NATO. It also contained a **cyber "table-top" exercise**, which was designed in order to verify the analytical thinking of the participants when facing real cyber threats and incidents and comparison of the reactions of each country. French observers from the **French National Agency for Information System Security (ANSSI)** also accepted the invitation to the Spring and Autumn Sessions of CECSP. Apart from two sessions of CECSP in Bratislava, the authority also initiated an **ad hoc meeting of liaison officers** for cybersecurity of the CECSP countries and France operating in Brussels. Its participants informed each other of the national positions regarding the current European topics of cybersecurity, whose trend determines the so-called cyber package.

BILATERAL RELATIONS

In 2017, the extension of the number of bilateral **agreements on the exchange and protection of classified information** continued and without these agreements the exchange of classified information, recognition of security clearance screenings issued abroad could not take place and the private sector could not participate in the implementation of contracts, where foreign classified information is forwarded. The authority as the responsible authority, addresses its partners abroad and prepares draft agreement texts approved by the Government of the Slovak Republic. In July 2017, the Government of the Slovak Republic approved the agreement with the **United Arab Emirates.**

In 2017, the authority managed to establish strategic relations in the cybersecurity field with the **French ANSSI**, which was supported by bilateral visits and participations of the ANSSI representatives in national and regional events organised by the authority in Slovakia. In 2017, he liaison officer of the authority within NATO became the liaison officer for communication with ANSSI. The collaboration possibilities between the authority and ANSSI opened mainly the areas of close involving mainly exchange of experience, sharing information, organisation of joint exercises and formulation of coordinated opinion concerning the cybersecurity agenda within the field of the EU and NATO.

The establishment of collaboration with Romania in the field of cybersecurity led in December 2017 to signing of a memorandum of understanding between the authority (as operator of the national SK-CERT) and the Romanian unit for solving cyber incidents (CERT-RO. The memorandum contained setting of the mechanisms for sharing information and reactions to cyber incidents.

EXCHANGE OF FOREIGN INFORMATION

Through the **central register** workplace, in 2017 6,721 pieces of classified information of NATO and 4,866 pieces of classified information of EU were processed. The authority intermediated also the exchange of 108 pieces of foreign classified information. The overview of central register in 2017 and comparison of data with 2015 and 2016 is included in Table No. 4.

Table No. 4: Exchange of classified documents in 2015 - 2017

Level of classification	2015	2016	2017
NATO Restricted	1,092	3,520	2,778
EU Restricted	970	1,449	4,453
Foreign - Restricted	12	35	84
NATO Confidential	1,287	1,890	1,576
EU Confidential	796	829	334
Foreign -Confidential	6	21	13
NATO Secret	1,050	1,235	2,367
EU Secret	88	92	79
Foreign - Secret	8	9	5
NATO Top Secret	0	0	0
EU Top Secret	0	0	0
Foreign - Top Secret	6	2	6
Total NATO	**3,429**	**6,645**	**6,721**
Total EU	**1,854**	**2,370**	**4,866**
Total Foreign	**32**	**67**	**108**

In the **NATO ATOMAL register** of classified information in 2017 there were two classified papers with classification marking NATO SECRET ATOMAL.

Important events of the past year also included the alliance exercise **NATO ABLE STAFF 2017,** which was to verify the procedures and communication systems related to nuclear planning and consultations, exercise the applicable measures of the NATO Crisis Response System (NCRS), carry out a practical training of staff at the NATO Headquarters, in the Supreme Headquarters of Allied Powers in Europe (SHAPE) and the national headquarters in consulting procedures. The authority participated in the exercise at the distributional level. Through the central register, it ensured receipt and forwarding to classified information. The communication during the exercise took place in the environment of the **NATO NNCCRS information system** (Nuclear Command Control Response System) managed by the authority in the Slovak Republic in order to ensure the information flow between the Slovak Republic and NATO in the field of nuclear planning.

3.3 PROTECTION OF CLASSIFIED INFORMATION

PERSONAL SECURITY

The performance of security clearance screenings of natural persons ranks among the key activities of the authority. In 2017, the authority issued **5,027 certificates for handling of classified information**, out of that 2,549 for the ministry of defence. The overview of the number of issued certificates in 2015 - 2017 is included in Table No. 5.

Table No. 5: Overview of certificates in 2015 - 2017

Level of classification	2015	2016	2017
Confidential	**2,104**	**2,316**	**3,060**
out of that Confidential for the Ministry of Defence of the Slovak Republic	499	558	1,308
Secret	**1,492**	**1,343**	**1,590**
out of that Secret for the Ministry of Defence of the Slovak Republic	909	866	1,029
Top Secret	**241**	**242**	**377**
out of that Top Secret for the Ministry of Defence of the Slovak Republic	150	109	212
Total	**3,837**	**3,901**	**5,027**

In 2017, the authority issued **28 decisions** and natural persons filed **12 appeals** against these decisions. The Committee of the National Council of the Slovak Republic for Review of the Decisions of the National Security Authority (hereinafter referred to as “authority”) discussed 15 appeals, while in 14 cases the appeals were dismissed, and in one case cancelled the decision of the authority and referred the case back to a new procedure. At the Supreme Court of the Slovak Republic (hereinafter referred to as “supreme court”) four actions were brought against the decision of the committee; out of that, one action was dismissed and three are in the decision-making process. Apart from the above mentioned, in 2017, the Supreme Court also decided in two proceedings, where the actions were filed in the previous period. In one case the Supreme Court cancelled the decision of the committee and referred the case back to a new procedure of the committee. In another case, the Supreme Court cancelled the decision of the committee as well as at the decision of the authority and referred the case back to a new procedure of the authority. The overview of the above mentioned information is included in Table No. 6.

Table No. 6: Appeals of natural persons against the decisions of the authority in 2015 - 2017

	2015	2016	2017
Decision of the authority	**54**	**36**	**28**
Appeals	**16**	**16**	**12**
Appeals dismissed by the committee	8	19	14
Decisions cancelled by the committee	1	0	1
Actions field at the Supreme Court	1	2	4

Based on the request of the Judicial Council of the Slovak Republic for **securing basic documents for decision-making on the preconditions for magistracy capacity of candidates (judicial vetting process) for appointment as judges,** in 2017 the authority provided the Judicial Council of the Slovak Republic with information to assess the eligibility of **69** candidates (51 in 2015 and 55 in 2016).

In relation to the **NATO and EU forwarded classified information,** in 2017 **5,261** certificates were issued to the proposed persons, out of that 2,648 NATO certificates and 2,613 EU certificates were issued. From the total number of NATO certificates, the authority issued 22 NATO ATOMAL certificates giving entitlement to access to information on the strategic nuclear deterrence of NATO and they are issued to a limited number of persons.

INDUSTRIAL SECURITY

In the field of industrial security, the authority performs **security clearance screenings of entrepreneurs.** The security clearance screening of entrepreneurs focuses on obtaining information on the entrepreneurs where there is a reasonable prospect that the state authority will ask them to create classified information or classified information will be forwarded to them. The obligation of the statutory body of the entrepreneur is in this case to apply to the authority to perform security clearance screening in order to obtain an **industrial security confirmation.**

In 2017, the authority issued **77 industrial security confirmations,** out of those three confirmations at the level of classification Restricted, 60 confirmations at the level of classification Confidential and 14 confirmations of the level of classification Secret. The overview is included in Table No. 7.

Table No. 7: The overview of industrial security confirmations issued in 2015 - 2017

Level of classification	2015	2016	2017
Restricted	13	5	3
Confidential	79	57	60
Secret	11	5	14
Top Secret	1	1	0
Total	**104**	**68**	**77**

In 2017, the authority issued **13 decisions.** Two entrepreneurs filed an appeal against the decision of the authority. In one case, the authority decided in interlocutory revision and in one of the appeal the committee took a decision, which dismissed the appeal of the entrepreneur. The overview of these decisions is included in Table No. 8.

In relation classified NATO and EU information, in 2017 **six NATO certificates and nine EU certificates** were issued to entrepreneurs authorising the entrepreneurs to handle NATO and EU classified information respectively.

Table No. 8: Appeals of entrepreneurs against the decisions of the authority in 2015 - 2017

	2015	2016	2017
Decision of the authority	**26**	**22**	**13**
Appeals	**2**	**6**	**2**
Appeals - interlocutory revision	1	1	1
Appeals dismissed by the committee	1	2	1
Decisions cancelled by the committee	0	1	0
Actions field at the supreme court	1	0	0

PHYSICAL SECURITY AND BUILDING SECURITY

Within the performance of security clearance screenings of entrepreneurs, in 2016 the authority assessed the measures of physical security and building security for the protection of classified information at **44 vetted entities** and issued **one consent to authorisation of the entrepreneur** to perform verification of conformity of mechanical barriers.

The authority issued **43 certificates** of mechanical barriers and technical security equipment, out of that 39 type certificates and four equipment certificates.

PROTECTION AGAINST UNWANTED ELECTROMAGNETIC RADIATION

Within the measures for protection of classified information against leakage via **unwanted electromagnetic radiation (UER),** in 2017 the authority performed measuring of technical equipment and means of cryptographic protection of information in a specialised Tempest laboratory and zone measuring of space. When handling the 33 delivered applicants for performing UER measuring, **798 measuring of technical equipment and CPI means**, based on which 138 components were categorised. Based on the results of **111 zone measurements,** the authority assessed 101 premises.

ADMINISTRATIVE SECURITY

In compliance with the Act on Protection of Classified Information, in 2017 the authority ensured **receipt of classified information** from one entity without a legal successor, **withdrawal of classified information** from an unauthorised person and took actions necessary for ensuring their protection. Within the framework of increasing the security awareness of professionals and lay public, the authority performed two half-day and several shorter trainings on the selected issues of administrative security.

In 2017, the authority **received and sent 3,733 classified documents.** The comparison of the number of documents registered in the **protocol of classified documents** is included in Table No. 9.

Table No. 9: The number of classified documents processed at the authority in 2015 - 2017

Level of classification	2015	2016	2017
Restricted	2,943	3,580	3,439
Confidential	222	224	290
Secret	6	12	4
Top Secret	0	0	0
Total	**3,171**	**3,816**	**3,733**

TRAINING AND VERIFICATION ACTIVITY

Within the framework of implementing the **Concept of Building Security Awareness** in the field of protection of classified information, in 2017 the authority continued with the series of **presentations and trainings focused on each security field.** During the year, 85 such events took place, where 708 persons participated (574 from state authorities and 134 from the private sector). The lecturers from the authority clarified the changes resulting from the amendment of the implementing regulations to the Act on Protection of Classified Information, they focused on solving actual problems resulting from the application practice, or provision of recommendations related to the procedure of entrepreneurs applying for the industrial security confirmation. There was also a preparation of the applicants for obtaining a confirmation on attending the examination of **security employee.** In 2017, the Authority issued 303 such confirmations.

3.4 CRYPTOGRAPHIC PROTECTION OF INFORMATION

CRYPTOGRAPHIC PROTECTION SYSTEM

The cryptographic protection system in the Slovak Republic is based on a verified structure of departmental cryptographic authorities and their close cooperation with the authority serving as the **central cryptographic authority.** In 2017, the authority provided for the **administration of systems and CPI means** operated at the authority and in the state administration authorities. It continuously ensured the operational requirements of the departments and provided them with related support, mainly **production and distribution of the national cryptographic material and consultancy regarding the maintenance** of systems and tools used.

In 2017, the authority implemented a project focused on the **Establishment of s Secure Communication System** serving for the exchange of foreign classified information, including secured communication of government officials. Within the project, a complete revision and rebuilding of the network of classified government connection took place, including the exchange of cryptographic equipment, whose architecture failed to meet the requirements for information system security and on 31 December 2017 the validity of the certificates confirming their capability to protect classified information terminated.

CRYPTOGRAPHIC PROTECTION CONCEPT

In January 2017, the Government of the Slovak Republic approved the **Concept of Cryptographic Information Protection for 2017 to 2020** elaborated by the authority in close cooperation with the departmental cryptographic authorities. The material with classification marking of Restricted, determines the further direction of the system in the mid-term horizon and defines the main tasks of each actor.

CERTIFICATION OF CRYPTOGRAPHIC AND TECHNICAL EQUIPMENT

In 2017, the Authority issued 13 certificates of the means of cryptographic protection of information. In the field of security of technical devices, the authority issued 50 certificates and 15 addenda.

ACCREDITATION OF COMMUNICATION AND INFORMATION SERVICES

The authority in relation to public regulated service provided by the global satellite navigation system established in the European Galileo programme, perform the task of **Local Security Accreditation Authority**. It indirectly participates hereby in the creation and approval of legal and technical standards in the field of protection of classified information and their mutual reconciliation with the security policies of the EU. In the territory of the Slovak Republic, the authority is responsible for the security accreditation and surveillance of entrepreneurs interested in providing their services within this program. In 2017, there were **two communication and information systems accredited** for handling NATO classified information.

3.5 CYBERSECURITY

In 2017, the authority took steps in the field of **positive affecting of cyber space security** in the Slovak Republic. The main priorities in 2017 included establishment of a legislative and institutional cybersecurity framework in the Slovak Republic and building technical and professional capabilities.

Regular sessions of the **Committee of the Security Council of the Slovak Republic for Cybersecurity** took place, whose task was mainly to evaluate the security situation in the Slovak Republic and in the world and submit proposals for measures to the Security Council of the Slovak Republic increasing protection and reducing the risks of cyber space threats.

NATIONAL UNIT OF CSIRT

The authority operates a **specialised SK-CERT workplace** serving as the **national CSIRT unit.** From this position, the authority provides services related to the management of security incidents, elimination of their consequences and following restoration of the activity of information services in cooperation with the owners and operators of these systems. The workplace was established by transformation of the former security and operational monitoring centre of SK CSIRC and in 2017 it **gained accreditation** of the University of Carnegie Mellon for using the CERT trademark in it its name.

The information of cybersecurity incidents were processed from open sources, internal information channels and from classified communication and information networks. The SK-CERT workplace cooperated with **NCIRC (NATO CIRC)** and with the uniform warning system of the **EU NSIAM** (European Union Network Security Incident Alert Mechanism).

The obtained information on threats and incidents, together with the proposals for countermeasures were sent by the authority to authorities and organisations included in the SK-CERT distribution list. When distributing to the government departments, the **Apeiron** communication information system and communication channels of the **National Security Analytical Centre (NBAC)** were used, where the authority served as a responsible entity for solving cyber threats.

BUILDING TECHNICAL AND PROFESSIONAL COMPETENCE

In 2017, the authority continued building technical competence, mainly by extending the hardware and software equipment necessary for accomplishment of the tasks within SK-CERT and the SOC (Security Operation Centre) workplace. An important aspect was preparation of the particulars and documentations, which did not only involve technical specifications but also setting of procedural rules and division of competencies of individual workers.

Within the **increase of professional expertise,** the representatives of the authority participated in national and international conferences, workshops and exercises. These activities were not only focused on obtaining experience and knowledge on new trends in the field of cybersecurity, but also served for establishing professional relationships with partners.

The prestigious exercises **Locked Shields 2017,** which is regularly organised by the NATO Centre of Excellence for cyber defence with its seat in Tallinn, Estonia, is one of the biggest in the world. It offers technically challenging scenarios focused on the training of experts in the field of cyber defence and security. In 2017, the representatives of the authority joined these exercises together with 800 other participants from 25 countries. At the **NATO Cyber Coalition 2017 exercise**, which verified the process, technical and communication skills of participants, the authority ensured surveillance through a local trainer. The authority also participated in the third year of the **CyberEx 2017** exercise organised by the Spanish National Institute for Cybersecurity (INCIBE) and the Organisation of American States (OAS). The goal of the exercise was, through solving a certain incident, to verify the ability of the participants to analyse cyber-attacks and to respond to them. The team consisting of representatives of the authority, National Agency for Utility and Electronic Services and of the ESET Company succeeded in the exercise and in very strong competition came as second.

BUILDING SECURITY AWARENESS

Within the **building of cybersecurity awareness**, the authority started to issue **security bulletins and warnings** focused on distribution of the most important information in the cyber security field. The bulletins were issued and sent out to partners on a weekly basis. Warnings were issued and sent out based on the need, mainly in case of critical vulnerabilities, serious incidents and threats. In December 2017, the **website of the specialised SK-CERT workplace was launched** (www.sk-cert.sk), which summarises all the necessary information in the field of cybersecurity. There are specialist articles, advice, instructions, and archive of security bulletins and warnings.

3.6 TRUST SERVICES

In compliance with the supervision scheme, the **authority performs supervision of qualified providers** of trust services. Ex post supervision is performed over the non-qualified providers of trust services, and that only in case if the authority obtains information that do not meet the requirements determined in the eIDAS Regulation.

The authority as **supervision body informed** the trust service providers and the public **on vulnerability of equipment** for execution of qualified electronic signatures. When evaluating the risk rate of overcoming the vulnerable keys, all the variables affecting the probability of their abuse were taken into consideration. The providers took adequate measures and the potentially vulnerable 2K and 4K keys were replaced by safer 3K keys.

TRUSTED LIST

The authority manages and publishes on its website a **trusted list** containing information **on provided qualified trust services**, which are under the supervision of the Slovak Republic and information on the provided **qualified trust services.** During 2017, the authority published 11 versions of the trusted list.

LIST OF AUTHORISATIONS

The list of authorisations, which is an **information source** for qualified providers or trust services for issuing **mandate certificates**, is published by the authority on its website. In 2017, based on the applications of state authorities and local authorities, 38 new authorisations were added to the list. During the year, the authority published 17 versions of the list of authorisations. Its current version was always completed with the archive of previous versions.

UNIFORM PROVISION OF TRUST SERVICES IN THE EU

On 1 July 2017 the transitional period finished, during which upon the provision of trust service it was allowed to use the (former) national solutions. The granting of qualified statute to a trust service and **provision of qualified trust services became uniform on the whole EU digital market.** If after the **termination of the transitional period,** the existing providers wanted to continue in providing their services, in the new terminology defined as qualified services with granted qualified statute, they had to undergo an audit, which was to show whether their services meet the requirements of the eIDAS Regulation. **Five providers of trust services** took this opportunity, to whom the authority confirmed the statute for the provision of qualified trust services of execution and verification of qualified certificates for **electronic signature / electronic stamp** and execution of qualified **electronic time stamps.**

NEW TRUST SERVICES

The authority received notices of four providers stating their interest in providing **new qualified trust services** (for example execution and verification of qualified certificates for the authentication of websites, validation of qualified electronic signatures / electronic stamps, maintenance of qualified electronic signatures / electronic stamps). The notice had to be submitted by the provisions together with the final report on conformity assessment.

The authority assessed and granted the applications of four providers for **extension of existing qualified services** with the OCSP service (Online Certificate Status Protocol) as of 1 January 2018. Based on the notice of one of the providers on the intention to terminate the provision of two services, the authority withdrew their qualified statute for these qualified trust services.

ROOT CERTIFICATION AUTHORITY

The authority operates the **root certification authority of the Slovak Republic** issuing certificates of public keys to qualified providers of trust services, i.e. accredited certification authorities, **issues certificates of public keys.** The authority is the operator of technology for maintaining the list of all issued qualified certificates containing the data on their validity. The authority provides this data upon demand.

In 2017, the authority **issued one certificate** for a qualified provider of trust services and **cancelled one certificate.** It issued a certificate for a qualified provider of trust services for the service of execution of qualified electronic time stamps and **issued 132 qualified certificates** for electronic stamps.

4. ECONOMY AND BUDGET

The National Council of the Slovak Republic approved the governmental bill of act on state budget for 2017 on 29 November 2016.

BREAKDOWN OF MANDATORY BUDGET INDICATORS

The breakdown of mandatory budget chapter 41 - National Security Authority, influence of budgetary measures on the level of budget as of 31 December 2017 and comparison of the drawdown of funds to the adjusted budget as of 31 December 2017 is included in Table No. 10.

Table No. 10: Budget of the authority for 2017

	Budget breakdown	Adjusted budget	Actual	Fulfilment to the adjusted
I Revenues of the chapter				
A. Mandatory indicator	€ 20,000.00	€ 20,000.00	€ 36,024.55	180.12%
B. Funds from EU budget	€ 0.00	€ 0.00	€ 0.00	–
II Total expenses of the chapter (A+B)	**€ 8,793,684.00**	**€ 16,924,473.12**	**€ 14,990,632.82**	**88.57%**
A. Total expenses without the European Union funds (600+700), out of that	**€ 8,793,684.00**	**€ 16,924,473.12**	**€ 14,990,632.82**	**88.57%**
A.1. Funds from the state budget - source code 111	€ 8,793,684.00	€ 8,835,550.68	€ 8,563,542.86	96.92%
- source code 131	€ 0.00	€ 8,088,922.44	€ 6,427,089.96	79.46%
A.2. Funds for co-financing	€ 0.00	€ 0.00	€ 0.00	-
A.3. Wages, salaries, service income and other personal compensations (610) - source code 111	€ 4,731,085.00	€ 4,892,206.00	€ 4,792,233.23	97.96%
- out of that apparatus of the central body	€ 4,731,085.00	€ 4,892,206.00	€ 4,792,233.23	97.96%
Number of employees according to Annex No. 1 to the Officer of the Government of the Slovak Republic No. 667/2010, out of that	241 persons	241 persons	210 persons*	87.14 %
- apparatus of the central body	241 persons	241 persons	210 persons*	87.14 %
A.4. capital expenses (700), without the funds for co-financing, out of that	€ 0.00	€ 8,150,254.12	€ 6,486,335.64	79.58 %
- source code 111	€ 0.00	€ 61,331.68	€ 59,245.68	96.60%
- source code 131F	€ 0.00	€ 4,393,522.44	€ 2,731,707.96	**62.18%**
- source code 131G	€ 0.00	€ 3,695,400.00	€ 3,695,382.00	100.00%
B. Funds from the European Union	**€ 0.00**	**€ 0.00**	**€ 0.00**	**-**
C. Expenses of the state budget for implementation of the programs of the Government of the Slovak Republic	**€ 8,198,023.00**	**€ 12,716,412.12**	**€ 10,798,227.39**	**84.92%**
0EK0U - Information technologies financed from the state budget - NSA	€ 595,661.00	€ 4,208,061.00	€ 4,192,405.43	**99.63%**
D. Systematisation of police officers in civil service: volume of funds for service income in civil service	€ 4,477,902.00	€ 4,631,810.00	€ 4,607,443.65	99.47%
number of total posts	216 persons	216 persons	190 persons*	87.96 %

* Number of employees as of 31 December 2017

The mandatory budget indicators of the authority were observed in 2017. The authority upon management of funds observed the principles of economy, efficiency and purposefulness upon the observance legislative regulations, mainly as far as the Act No. 523/2004 Coll. on budgetary rules of public administration, resolutions of the of Government of the Slovak Republic and methodical instructions and guidelines of the Ministry of Finance of the Slovak Republic are concerned.

BUDGET FOR 2018

The Act on State Budget for 2018 was approved by the National Council of the Slovak Republic on 13 December 2017. Following item C.1 of the Resolution of the Government of the Slovak Republic No. 471/2017 to the draft public administration budget for 2018 to 2020 and provision of the Act No. 523/2004 Coll. on budgetary rules, the mandatory indicators for 2018 were announced to the authority. The expenses of the authority for 2018 were budgeted in the total sum of EUR 9,051,351.00, out of that EUR 8,466,513.00 within the program 0D9 - Information Security and EUR 584,838.00 within the interdepartmental program OEKOU - Information technologies financed from the state budget - NSA. The income is budgeted in the sum of EUR 20,000.00.

The budgetary funds will be used by the authority upon accomplishment of the tasks resulting from the generally binding legal regulations and resulting from the obligations of the Slovak Republic towards the EU and NATO.

5. INSPECTION AND AUDIT

The inspection and audit activities is often perceived by the auditees as an unpleasant and repressive activity, although it also has a preventive and educative 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.

PROTECTION OF CLASSIFIED INFORMATION

In the field of classified information, in 2017 the authority performed **22 planned external inspections**, out of those 16 inspections in state authorities and six inspections in entrepreneurial entities. The inspection groups focused mainly on comprehensiveness of the adopted protection measures and their coordination throughout each field of security. **Deficiencies were identified in three inspected entities.** In the case of the first entity, the measures concerned the field of personal security and administrative security, in the second entity there were deficiencies found in the field of personal security and physical security and building security, and in the third entity there were deficiencies found in the field of administrative security. In total **12 deficiencies** were discovered - nine in the field of administrative security, two in the field administrative security, two in the field of personal security and one in the field of physical security and building security.

In 2017, **four inspections were performed beyond the framework of the approved inspection plan** in state administration authorities. The actual state administration authorities applied to the authority and requested their performance, or they were performed based on a motion. **Deficiencies were identified in one entity.** They concerned the measures in the field of administrative security (13 deficiencies), personal security (3 deficiencies) and physical security and building security (1 deficiency).

In general, the inspections performed confirmed the tendency to reduction of the number of deficiencies found. This trend confirms that the assurance of protection of classified information approaches the desired level.

AUTHORISED PERSONS

In 2017, the authority performed **four planned inspections of authorised persons,** which were focused on verification of meeting the statutory conditions and conditions specified in the consent to authorisation. **Two state authorities** authorised for certification of technical equipment and **two entrepreneurial entities** authorised for execution of verification of the conformity of mechanical barriers and technical security equipment with the respective security standards underwent the inspection. During the inspections, **no violation** of the generally binding legal regulations **was identified**.

INTERNAL INSPECTION AND AUDIT

The internal inspection bodies in 2017 performed **nine internal inspections.** The four performed inspections concerned material accomplishment of tasks from the government resolutions. Other inspections were mainly focused on the inspection of the protection of classified information in the field of security of technical devices, inspecting the condition of fire prevention, inspecting adherence to the operating rules and performance of physical protection of the authority and inspecting the state of OHS in the field of performing the security and technical service. During the inspections, **no violation** of the generally binding legal regulations **was identified**.

In 2016, there were **four internal audits** performed at the authority. They were focused on verification and assessment of the use of state assets managed by the authority, fulfilment of the authority budget according to the program structure, using public funds for trainings and seminars, procedures of the authority according to the Act No. 9/2010 Coll. on complaints.

One **audit showed violation** of the obligations resulting from the internal regulations of the authority on purpose-built equipment of the authority. It was a deficiency of low relevance, which is systematically and financially incalculable. Consequently, measures to remedy the identified deficiencies and for elimination of the reasons for their occurrence were adopted.

6. CONCLUSIONS AND PRIORITIES FOR 2018

Year 2017 was reach in events, which had a direct impact on the status, operation and perception of the authority. The activities of the authority included accomplishment of a wide spectre of tasks. They were mainly focused on the individual aspects of applying new competences, which result from its position of a central state administration body for cybersecurity.

The activity of the authority in the field of **protection of classified information** in 2017 was not limited by any extraordinary events or circumstances, which would have a negative impact on the quality of performing the activities related to the performance of **security clearance screenings** of natural persons and entrepreneurs, **certification** of technical equipment, mechanical barriers and technical security equipment, protection of **foreign classified information and inspection activity.**

During the year, works on the preparation of the new **Act on Protection of classified Information** continued, which is to determine the optimum principles and minimum standards for creation of a secure environment for classified information. **In 2018**, the authority plans to **submit the act into the legislative process**.

In 2017, the authority implemented an important project of **secure communication system** for the exchange of foreign classified information, which also included restructuring of the secured network of **classified communication of government officials.** In 2018, within the framework of the project, **computerisation of the** foreign classified information will continue, as well as their online connection with the registers of public administration authorities. Hereby the preconditions were created for full **elimination of paper-based classified information, simplification of their registration** and substantial **speed up upon their exchange.** The authority will continue development of the **cryptographic information protection system** and its adaptation to the Android operation system.

On **1 July 2017, the transitional period terminated,** during which the EU member states were enabled to use their national solutions **upon the provision of trust services.** The granting of qualified statute to a trust service and **provision of qualified trust services became uniform on the whole EU digital market.**

In 2017, the works in preparation of the Act on Cybersecurity were completed. **Act No. 69/2018 Coll. on cybersecurity came into force on 1 April 2018.** Act comprehensively covers the agenda of solving and ensuring security in the national cyber space and creates a **wider competence base** for the authority in the field of cybersecurity and **defines the rights and obligations** of each entity.

In 2017, the authority continued **building technical competences** in the field of cybersecurity. Extension of the hardware and software equipment, setting of procedural rules, preparation of technical specifications and documentation of the **Security Operations Centre (SOC) and of the specialised SK-CERT workplace** rank among the necessary preconditions for ensuring the services connected with management of security incidents, elimination of their consequences and following restoration of the activity of information systems. In 2018, **the process SK-CERT certification will be completed** by issuing the internationally valid certificates **FIRST** and **Trusted Introducer** forming the condition for obtaining membership in these renowned organisations. Membership is not only the matter of prestige, but it also brings attractive benefits, mainly sharing of cyber-relevant information, exchange of knowledge and experience.

In 2017, there was a **significant increase** of authority activities focused on the **development of bilateral, regional and multinational cooperation.** The authority managed to establish several **strategic bilateral partnerships. Excellent cooperation** within the **Central European region** was a stepping-stone for **coordination of procedures** and formulation of joint opinions of the V4 countries, Austria and France on the draft strategic documents and legislative acts **within the EU and NATO.** Participation in national and international **conferences, workshops and exercises** brought precious experience and knowledge of new trends in the field of cybersecurity and served for establishing relations with partners.

Within the **building of cybersecurity awareness**, the authority started to issue **security bulletins and warnings** focused on distribution of the most important information in the cyber security field. In December 2017, the **website of SK-CERT was launched**, which summarises all the necessary information in the field of cybersecurity. In the field of building the security awareness, in 2018 the authority will concentrate on **more detailed elaboration of communication topics** and definition of more targeted messages intended for **individual target groups.**

Within the **European operational program Science and Innovations,** the authority is preparing a national project of long-term strategic research in the field of cryptographic protection and cybersecurity. The project will be solved **in partnership with the university sector.** The project assumes **building of a national Public Key Infrastructure (PKI),** which will be enriched by new and more secure algorithms, faster and more efficient cryptographic equipment and more secure application programs. The project will focus on **increasing of resistance and fine-tuning of systems** and protection of classified information using cryptographic means.

In 2017, the authority joined the **National Quality Program of the Slovak Republic.** Within the framework of the Improvement Strategy of Product and Service Quality by Organisation Improvement 2017-2021, which defines the basic directions for quality improvement in organisations of the public and private sector, the authority with implement the **CAF model** in the coming years as a tool of total quality management.