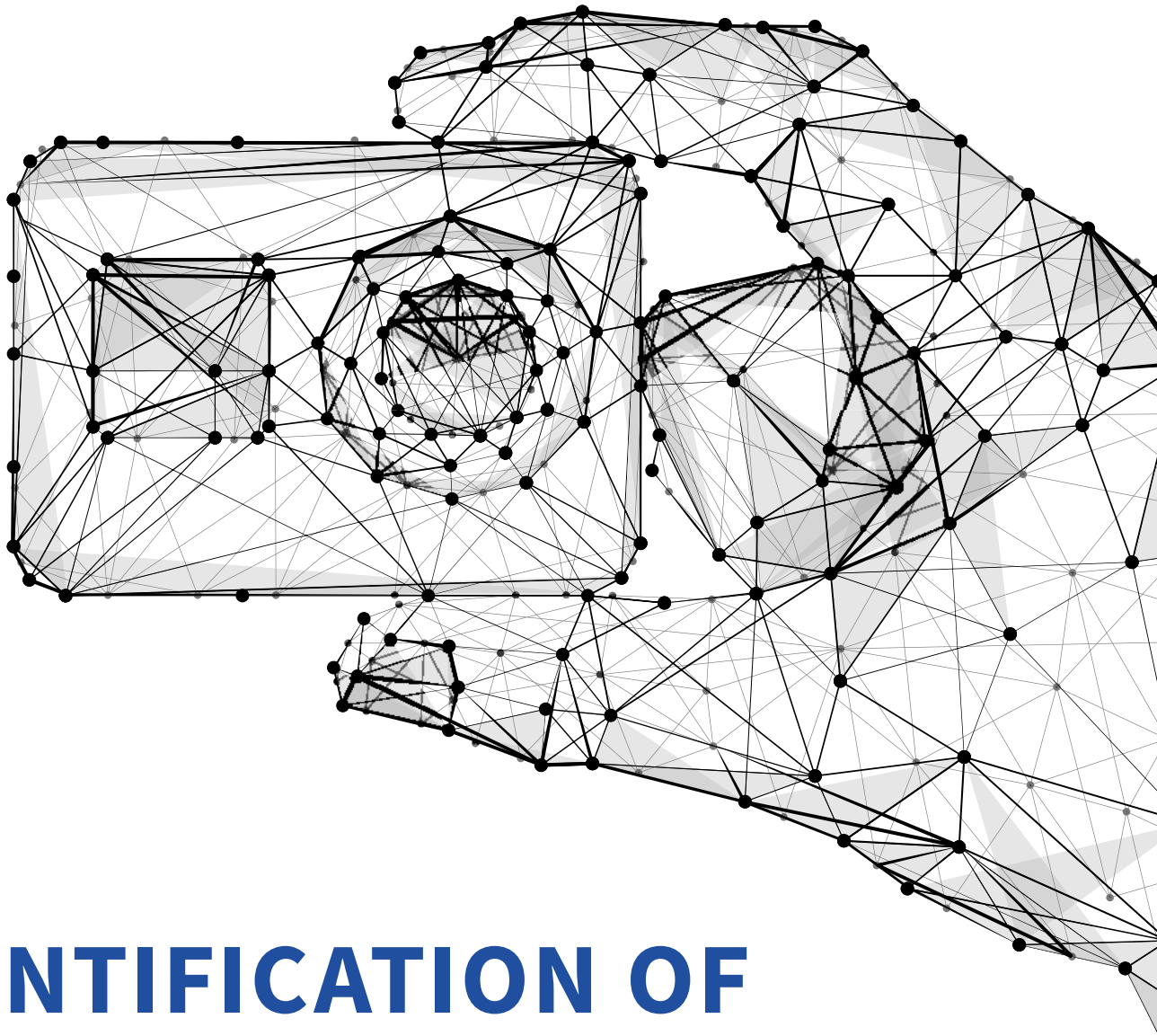
NATIONAL SECURITY AUTHORITY

REPORT ON ACTIVITIES IN 2023

NATIONAL SECURITY AUTHORITY

REPORT ON ACTIVITIES IN 2023

CONTENTS

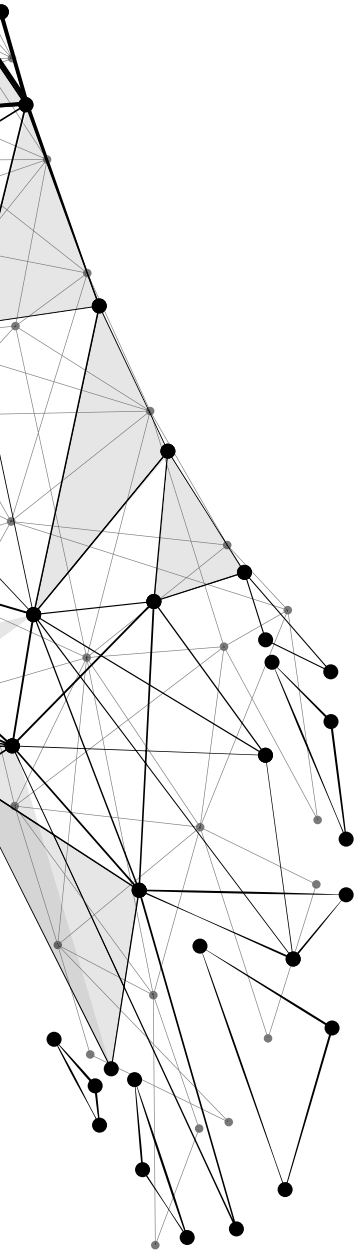


IDENTIFICATION OF THE ORGANIZATION

The National Security Office (Národný bezpečnostný úrad - NBÚ) is responsible for creating and implementing state policy in the areas of protection of classified information, cybersecurity, encryption services, and trusted services. In the area of classified information protection, it conducts security clearances for individuals and businesses, provides opinions on proposed individuals according to international treaties binding on the Slovak Republic, and maintains records related to the protection of classified information.

It certifies communication and information systems for handling classified information, issues approvals for the authorization of state bodies or businesses to certify technical means, and performs conformity verification of mechanical barriers and technical security measures with security standards; it also conducts certification of technical, system, mechanical barriers, and technical security measures.

The office assesses the conditions at businesses and state bodies, including the assessment of the protection of exchanged classified information and the conditions for protection against unwanted electromagnetic emissions from technical means and encryption protection tools.



The office ensures the management and operation of the entrusted information systems, including user account management, the management and operation of classified governmental and foreign communications systems, and performs security oversight of the network and application parameters of communication and information systems for the protection of classified information.

Through its internal control activities, the office verifies the conditions for ensuring the protection of classified information in state and local government bodies as well as in businesses, and issues methodological guidance on various aspects of classified information security.

The office also carries out activities that enhance security awareness and conducts examinations for security personnel.

In the international exchange of classified information, the office functions as the central register for the exchange of classified information in the Slovak Republic and participates in the protection of foreign information.

In the area of regulation and methodology, the office issues security standards, opinions, and methodologies for generally binding legal regulations and documents that fall within the office's remit, prepares proposals for generally binding legal regulations for the legislative process, comments on, and prepares opinions on draft legislative materials during inter-ministerial comment procedures.

Methodological guidance is provided by the office to state bodies, businesses, and individuals in all areas of its remit. The office also publishes anonymized methodologies and expert opinions on the office's website.

In the area of encryption protection, the office fulfills the tasks of the central encryption authority of the Slovak Republic. It certifies encryption tools, issues security standards, and coordinates research and development of encryption protection tools.

Lastly, the office acts as the national authority in international cooperation and ensures the function of the National Distribution Authority, which is the entry and contact point of the Slovak Republic for the exchange and distribution of encryption protection tools and encryption materials through the National Distribution Authority and fulfills the tasks of the National Distribution Authority for the distribution of NATO and EU COMSEC material. In the area of trusted services, the office functions as a supervisory authority. It performs tasks related to the granting and revocation of qualified status for services provided by qualified trusted service providers, which it publishes in the trusted list containing information about trusted services.

It also oversees the certification of devices for creating qualified electronic signatures and qualified electronic seals; it creates, maintains, and publishes a list of mandates for the issuance of mandate certificates.

The office also operates the Root Certification Authority of the Slovak Republic, which maintains a database of expired qualified certificates issued by providers under the office's supervision, and provides unlimited information on their validity during their usage period; it allows qualified trusted service providers to issue public key certificates.

In the area of cybersecurity, the office is the national authority for cybersecurity.

It manages and coordinates the performance of state administration in the area of cybersecurity, sets standards, and issues policies for behavior in cyberspace.

The office is the national body for cybersecurity certification according to European cybersecurity certification schemes. For the level of "high" assurance, it is the sole certification body according to the relevant schemes.

The office is the main point of contact for foreign affairs in the area of cybersecurity, cooperates with central authorities, operators of essential services, and providers of digital services, accredits CSIRT units, and cooperates with analytical security centers for the exchange and sharing of information on security incidents.

KEY LEGAL REGULATIONS

- Act No. 215/2004 on the Protection of Classified Information, related decrees, and applicable standards.
- Act No. 272/2016 on Trusted Services for Electronic Transactions in the Internal Market.
- Act No. 69/2018 on Cybersecurity and its decrees. Relevant and related international, European, and national legal regulations.

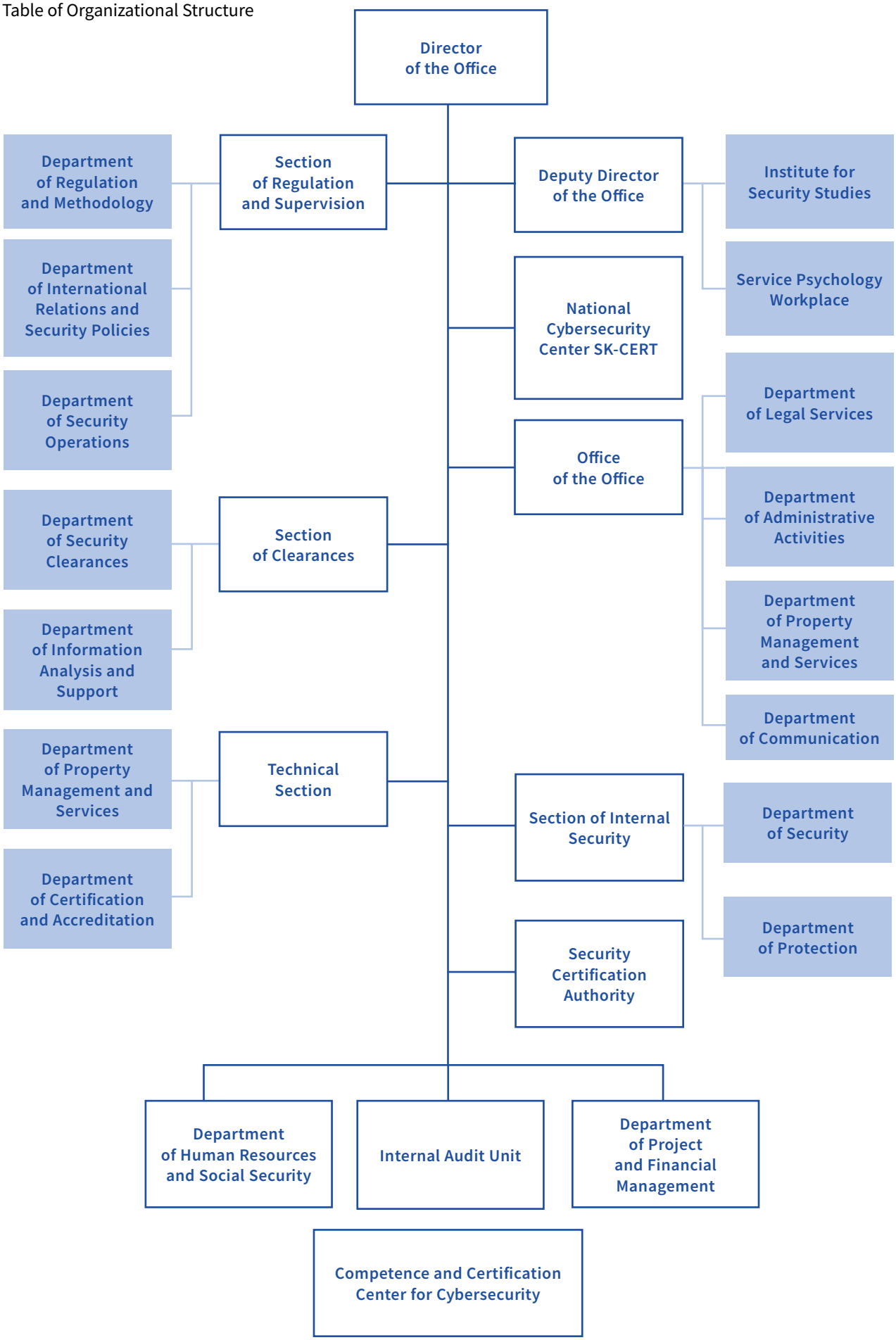
LEADERSHIP OF THE OFFICE

The office is headed by a director, who is responsible for its activities. The director manages and represents the office externally. The director decides on the implementation of the office's main tasks, approves internal legal regulations, decides on the internal organizational structure, and personnel matters of the office's members and employees. The director oversees inter-ministerial cooperation and is a permanent invited member of the Security Council of the Slovak Republic.

The director sets the principles of the office's international cooperation and, in accordance with the foreign policy priorities of the Slovak government, supports and develops partnerships with institutions of foreign states and international organizations. In the director's absence, the deputy director of the office, who is also responsible for coordinating the activities of the office's units, acts within the scope designated.

ORGANIZATIONAL STRUCTURE

Table of Organizational Structure



DEPARTMENTS OF THE OFFICE

Office of the Office

Coordinates the activities of the office's units, ensures and performs basic administrative and organizational activities related to the management and activities of the office, ensures legislative and legal matters of the office, builds and develops external relations and cooperation, and ensures communication with the public.

Clearance Section

Conducts security clearances of individuals and legal entities. In addition to certificates and confirmations that allow access to national classified information, it ensures the issuance of security clearance certificates for individuals and certificates of industrial security for entrepreneurs for handling NATO and EU classified information and provides opinions on proposed individuals according to international treaties binding on the Slovak Republic.

SVB — Section of Regulation and Supervision

This is the office's unit responsible for the protection of classified information, encryption protection of information, cybersecurity, trusted services, and the public regulated service provided by the global satellite navigation system established in the Galileo program.

It fulfills tasks in the area of control, audit, and supervision. It grants and revokes qualified status, determines the essential service and its operator, and determines the digital service and its provider.

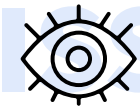
It issues opinions and methodologies, creates conceptual and strategic materials, and develops security and knowledge standards, whose established procedures are incorporated into international standards through ISO working groups or European standardization institutions. It issues certification and signature policies.

It organizes and conducts security personnel exams and training in the area of classified information protection.

At the international level, it represents the office and coordinates the office's foreign activities. It comments on draft legislative materials in the inter-ministerial comment procedure and conducts the legislative process for materials with an international element.

Its liaison officers in the EU, NATO, and the USA fulfill tasks related to developing and building the office's international relations and cooperation abroad. They ensure communication between the office and foreign partners and represent the interests of the Slovak Republic.

Internal Security Section



The Internal Security Section ensures the internal security of the office, fulfills tasks in the area of classified information protection, ensures the physical and technical protection of the office's premises, the office's director, and the office's employees.

In the area of internal security, it gathers, analyzes, and verifies information about security risks concerning the office's activities, members, and employees. It investigates offenses in areas under the office's jurisdiction.

It conducts internal control, handles complaints and petitions, and fulfills the role of a responsible person in handling reports of anti-social activities, in the area of personal data protection, and in the area of corruption prevention. It fulfills tasks in the area of occupational health and safety, fire protection, and ensures the professional preparation of members.

Technical Section

The Technical Section consists of the Department of Security Operations and the Department of Certification and Accreditation.

It conducts accreditation and certification in the area of classified information protection for personnel security, administrative security, physical security, object security, technical means security, and industrial security, in the area of encryption protection of information, in the area of cybersecurity, and in the area of trusted services.

It manages and operates the office's information and communication systems, manages and operates classified government and foreign communication systems. It also conducts security oversight of the network and application parameters of communication and information systems for the protection of classified information.

National Cybersecurity Center SK-CERT

It fulfills the tasks of the national CSIRT unit. It provides services related to managing security incidents, mitigating their impacts, and restoring the function of information systems in cooperation with their owners and operators, as well as performing analytical tasks, research, security awareness-raising, and education in the area of cybersecurity and other tasks in the area of cybersecurity.

Department of Human Resources and Social Security

It implements the office's personnel and payroll policy, social security, education, and remuneration. It coordinates healthcare for the office's members and employees.

Department of Project and Financial Management

It ensures project and program management within the office.

Internal Audit Unit

It conducts internal audits of the office and fulfills other tasks according to the law on financial control and audit.

Institute for Security Studies

It fulfills tasks in the area of general analytics, security risk assessment, policy evaluation, development of forecasts, strategies, and implementation plans of the office, as well as tasks in the area of combating hybrid threats and the spread of disinformation.

Security Certification Authority

The Security Certification Authority is a substantive unit of the office that fulfills the role of the national certification authority for cybersecurity according to a specific regulation.

Competence and Certification Center for Cybersecurity

The Competence and Certification Center for Cybersecurity is a contributory organization of the office that, in the public interest, helps fulfill the office's professional tasks in the area of cybersecurity, protection of classified information, encryption protection, and trusted services.

HUMAN RESOURCES

Overview of the number and structure of members and employees

	State Service		employees		totaling	
Preparatory state service	**37**	16,8 %				
Permanent state service	**176**	80 %				
Temporary state service	**7**	3,2 %				
Total	**220**	92,8 %	**17**	7,2 %	**237**	100 %

Age structure of members and employees

	members		employees		totaling	
Up to 34 years old	46	20,9 %	4	23,5 %	50	21,1 %
35 to 49 years old	117	53,2 %	7	41,2 %	124	52,3 %
50 to 59 years old	48	21,8 %	3	17,7 %	51	21,5 %
60 years and above	9	4,1 %	3	17,7 %	12	5,1 %
Total	220	90,4 %	17	9,6 %	237	100 %

Women and Men in NBÚ

	members		employees		totaling	
Women	103	94,5 %	6	5,5 %	109	46 %
Men	117	91,4 %	11	8,6 %	128	54 %
Total	220	92,8 %	17	7,2 %	237	100 %

Educational structure of members and employees

members			employees	
0	0 %	Basic education	0	0 %
36	16,4 %	Complete secondary education	7	41,2 %
8	3,6 %	University education (1st level):	0	0 %
164	74,5 %	University education (2nd level):	10	58,8 %
12	5,5 %	University education (3rd level):	0	0 %
220	100 %	Total:	17	100 %

SERVICE TRAINING

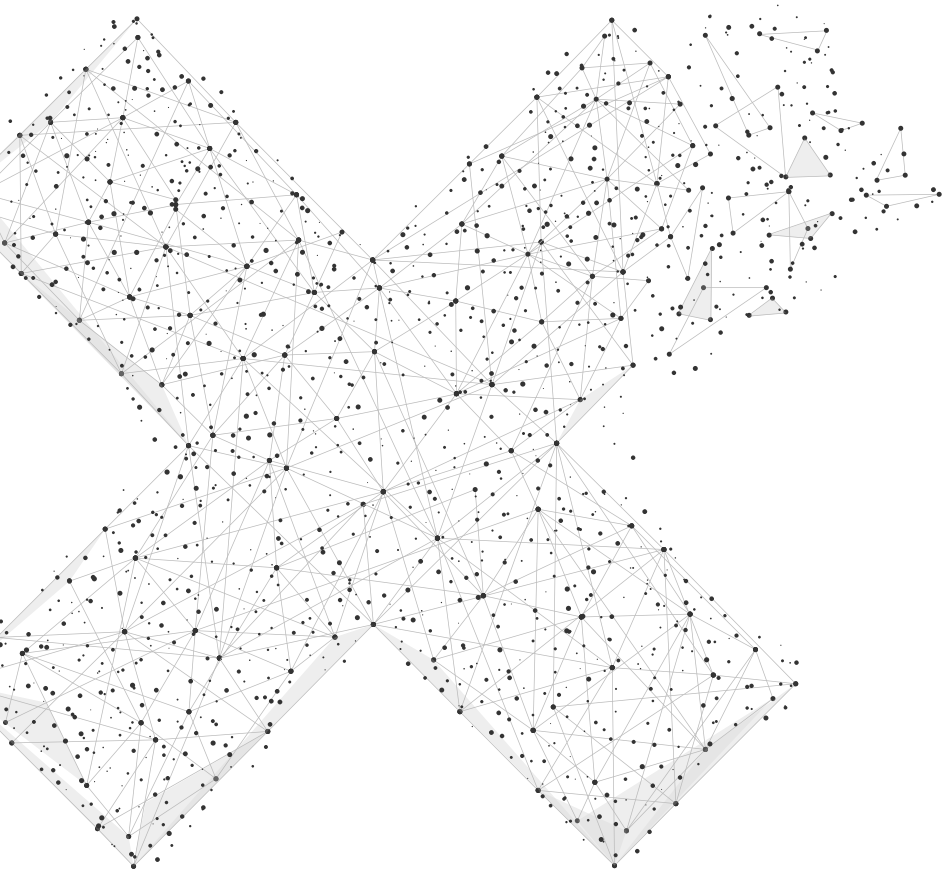
Members of the Internal Security Section fulfilled their tasks within service training through exercises in physical training, shooting training, special training, and medical training. They use facilities of armed security forces, armed forces, the Slovak Information Service, or the armed forces of the Slovak Republic for shooting and special training.

SERVICE PSYCHOLOGY WORKPLACE

The service psychologist conducted 59 psychological examinations of applicants for admission to the service of NBÚ members during 2023, of which 57 were concluded by the end of the year, with a success rate of 79%. The psychologist also conducted 4 traffic-psychological examinations, 2 analyses to map the current situation in selected units, and provided more than 140 hours of psychological counseling.

ENHANCEMENT OF QUALIFICATION AND SKILLS

The office allows its members and employees to maintain their professional readiness, acquire new skills, and deepen their qualifications through specialized courses, seminars, and training both at home and abroad.



FIGHT AGAINST CORRUPTION

In 2023, the office updated its Anti-Corruption Program, which is published on its website. The updated program aims to educate members and employees of the office about anti-corruption legislation at both the national and international levels, as well as educate them on internal regulations governing the office's anti-corruption measures. The goal is to create, implement, maintain, review, and improve the office's anti-corruption management system in accordance with the requirements of the ISO 37001 Anti-Bribery Management Systems standard.

In 2023, specialized training for members of the office included education on reporting under Act No. 54/2019 on the Protection of Whistleblowers of Anti-Social Activities.

In the area of corruption prevention, the office assessed the reliability of partners in substantive relationships, including a so-called anti-corruption clause in contracts with such entities. The office also initiated discussions on potential collaboration with third parties in the field of prevention and the fight against corruption, continuing its cooperation with the Government Office of the Slovak Republic and the Office for the Protection of Whistleblowers.

LEGISLATION

The National Security Office continued the systematic collection, analysis, and evaluation of information from the activities of the office's departments, from feedback from the professional public, or from requests for expert opinions. It harmonized national legal regulations with internationally recognized sources of law.

The office initiated six legislative processes for implementing regulations under Act No. 215/2004 on the Protection of Classified Information. The reasons were mainly new threats arising from global conflicts and continuous technological development.

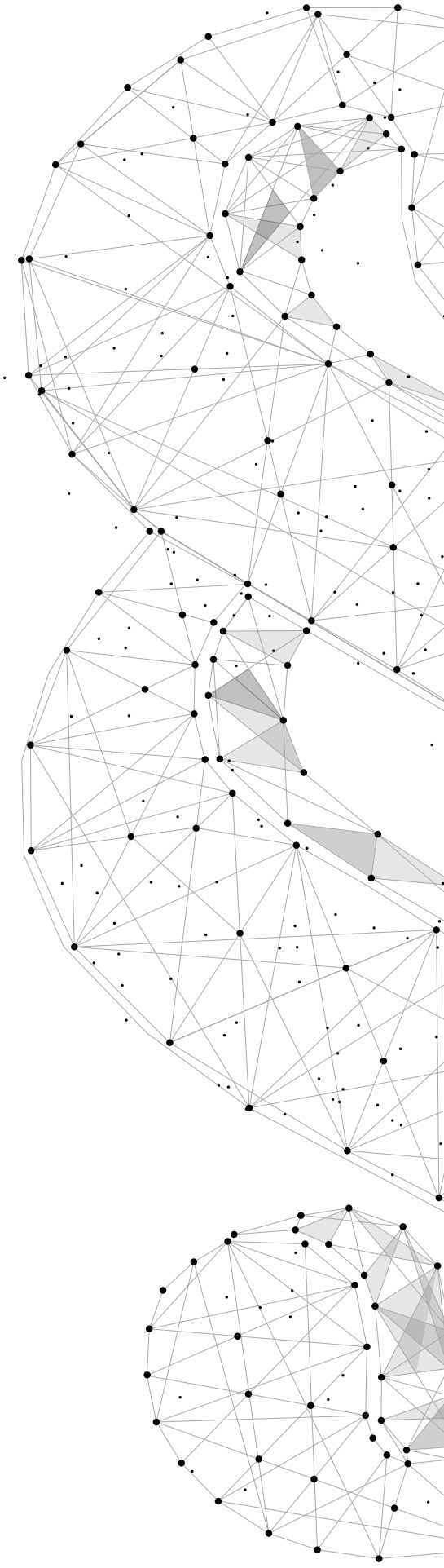
A draft of a new decree by the National Security Office on the examination of security personnel – preliminary information was published in March 2023. The aim of the draft is to ensure a higher level of security awareness among individuals responsible for the protection of classified information within entities or who perform specific tasks in this area (adjustment of the validity periods for the security personnel examination, the obligation to regularly verify professional competence). The draft is under internal review to be submitted for inter-ministerial commentary.

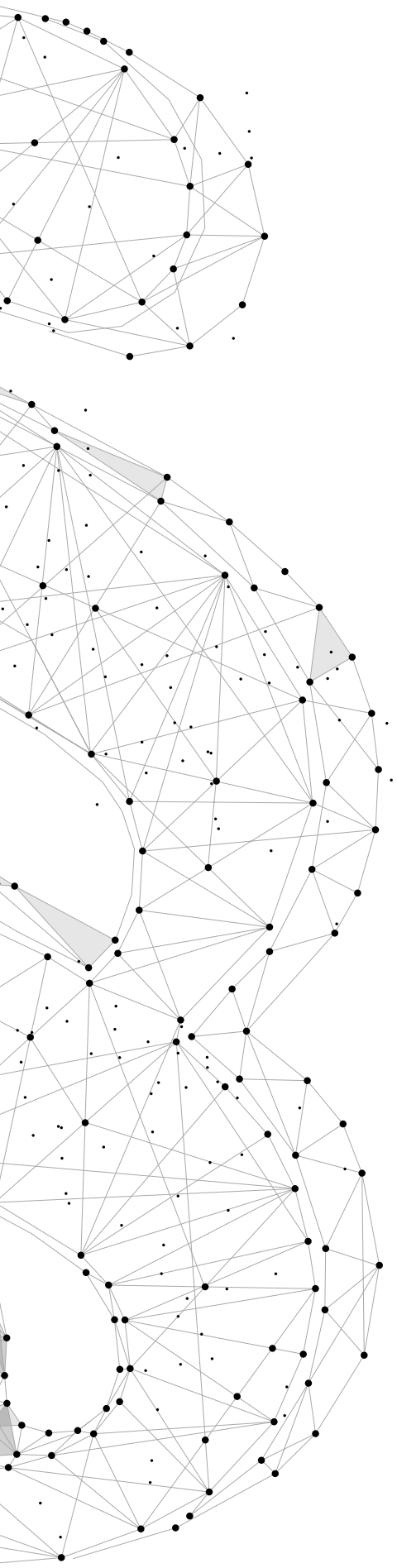
An amendment to NBÚ Decree No. 301/2013 on Industrial Security and the Security Project of Entrepreneurs – preliminary information was published in March 2023. The aim of the decree is to refine provisions on industrial security certificates for entrepreneurs, particularly those governing the procedure for recognizing certificates of foreign entrepreneurs or vice versa, thereby supporting the fulfillment of international treaties and obligations.

It is proposed to supplement the institute of certificate verification and the procedure for issuing certificates in the event of data changes. This adjustment will allow entrepreneurs to respond to changes in the legal form of their business. The amendment is under internal review to be submitted for inter-ministerial commentary.

An amendment to NBÚ Decree No. 134/2016 on Personnel Security – preliminary information was published in March 2023. The aim of the amendment is to refine certain provisions related to conducting security clearances, establish procedures for recognizing foreign security clearances, and details about certification. The draft amendment is being continuously adjusted to be submitted for inter-ministerial commentary.

An amendment to NBÚ Decree No. 48/2019, which regulates details on administrative security – preliminary information was published in March 2023. The aim of the amendment is to respond to findings arising from practical application and eliminate ambiguities that hinder clear interpretation or create obstacles in achieving the purpose, which is to ensure sufficient traceability of handling classified information.





In accordance with EU and NATO regulations and considering the damage caused by unauthorized handling, it is proposed to reduce the administrative burden on handling classified information at the Restricted level.

The new security situation that arose on the eastern border of the Slovak Republic in February 2022 prompted the administrative securing of the protection of a special category of classified information (such as defense industry products, ammunition, etc.). The proposal also refines the institute of unauthorized handling, which is not sufficiently regulated in the current legal framework.

The draft amendment is being continuously adjusted to be submitted for inter-ministerial commentary.

An amendment to NBÚ Decree No. 336/2004 on Physical Security and Object Security – preliminary information was published in March 2023. The aim is to include in the security standard a point-based evaluation for the use of certified encryption tools to protect classified information when stored instead of storing them in a security storage facility.

In accordance with EU and NATO regulations, an administrative zone will be added to Slovak legislation as a specific type of protected space in the Restricted category. It is proposed to add the possibility of storing classified information at the Restricted level in lockable furniture within a protected space, including the possibility of accounting for point-based evaluation for such storage.

The security documentation for physical security and object security of objects and protected spaces in the Confidential category will also be adjusted by expanding the content requirements to the level of security documentation for objects and protected spaces in the Secret and Top Secret categories.

In the process of preparing this proposal, a shortened legislative process was carried out at the urgent request of the Ministry of Defense of the Slovak Republic for the urgent amendment of NBÚ Decree No. 336/2004 on Physical Security and Object Security.

This involved the urgent addition of an exception only in connection with the protection of defense industry products, weapons, weapon systems, or ammunition that are either classified information or contain classified information transferred to the Slovak Republic by a foreign power. The Ministry of Defense of the Slovak Republic has long declared problems with the application of valid legislation in connection with the modernization of the armed forces.

The required changes necessitate extensive amendments to several legal regulations. The urgent amendment (NBÚ Decree No. 233/2023) came into effect on June 27, 2023.

The process for the new regulation of the Government of the Slovak Republic, which establishes areas of classified information – was submitted for inter-ministerial commentary in July 2023. The main aim of the proposed regulation is to update the

areas of classified information in the Slovak Republic, thereby responding to the needs of the state and its protected interests.

The aim is also to establish a mechanism for regulating public authorities when determining levels of classification and, in accordance with EU and NATO regulations, ensure the reconsideration of assigning the lowest level of classification (Restricted) to classified information, as unauthorized handling of such information may “only” result in damage to the legally protected interests of a legal or natural person.

As in 2022, the paradox was confirmed that other public authorities are requesting stricter protection of classified information at the Restricted level.

Another legislative activity of the office in 2023 was the initiation of the process for two implementing regulations to Act No. 69/2018 on Cybersecurity.

An amendment to NBÚ Decree No. 165/2018, which sets identification criteria for individual categories of serious cybersecurity incidents and details the reporting of cybersecurity incidents – preliminary information was published in February 2023.

The aim of the amendment is to clearly define criteria for identifying serious cybersecurity incidents. The decree introduces a standardized vulnerability assessment system representing a unified method for expressing the technical characteristics of vulnerabilities in hardware, software, firmware, and a numerical evaluation of their severity. The amendment is currently under internal review.

An amendment to NBÚ Decree No. 362/2018 Z. z., which establishes the content of security measures, the content and structure of security documentation, and the scope of general security measures (NBÚ Decree No. 264/2023) came into effect on September 1, 2023.

The aim of the amendment is to create a functional legislative framework necessary for the effective implementation of key measures for the security of the national cybersecurity space, transposing priorities and requirements established at the European level. This framework focuses on expanding the content of security measures, the content and structure of security documentation, and the scope of general security measures.

The Ministry of Justice of the Slovak Republic submitted a draft amendment to the Ministry of Justice Decree No. 228/2018, which implements Act No. 382/2004 on Experts, Interpreters, and Translators, for inter-ministerial commentary.

The office made a fundamental comment and requested the addition of the field of cybersecurity to the List of Expert Fields and Specializations, as well as to the Content Delimitation of Expert Fields and Specializations, and also to the List of Fields and Specializations where successful completion of specialized education is a condition for registration. The comment was accepted, and the amendment (Ministry of Justice Decree No. 160/2023) came into effect on July 1, 2023.

In addition to the above tasks in the field of legislation, the office comments on and prepares opinions on draft legislative and non-legislative materials during the inter-ministerial commentary process. The office reviewed 700 commentary procedures.

ADMINISTRATIVE AND OFFENSE PROCEEDINGS

NBÚ recorded 18 submissions regarding suspected offenses in the area of classified information protection under Act No. 215/2004 on the Protection of Classified Information.

- 1 case = a report on the result of the offense clarification was submitted to the competent administrative authority after identifying the perpetrator.
- 1 case = a matter concerning 1 of the 2 acts in the submission was handed over to the competent authority.
- 7 cases = the department clarifying the offense archived the matter with a record.
- 10 cases = the matter is still being clarified.

In 2023, we recorded 17 notifications of unauthorized handling of classified information.

In 2 cases, the matter recorded as unauthorized handling of classified information is being investigated by the competent authority in criminal proceedings.

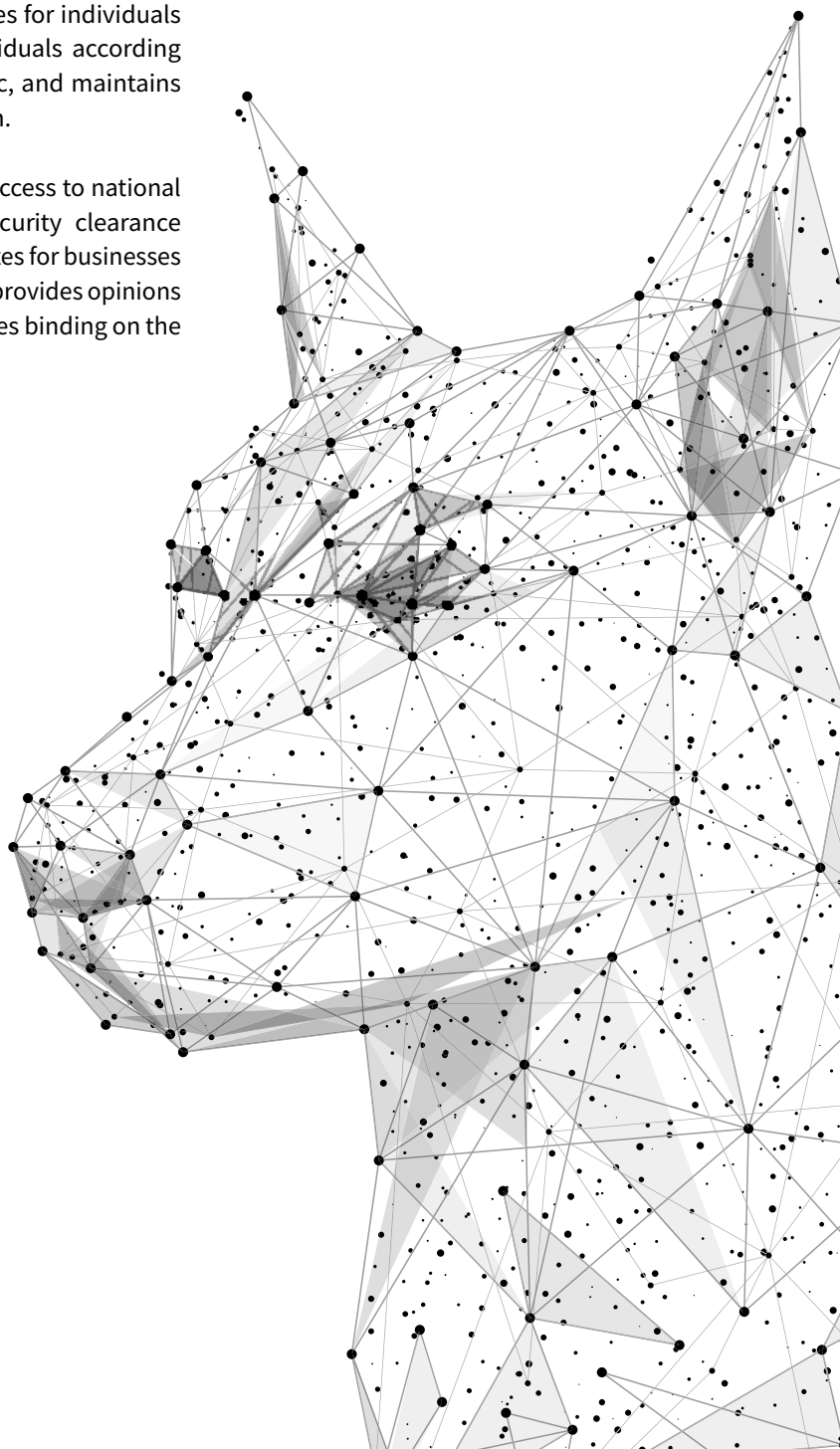
CONTRACTS FOR THE HANDLING OF CLASSIFIED INFORMATION

The office has a total of 13 contracts with entrepreneurs for access to classified information, with 1 contract and 4 amendments to existing contracts concluded last year.

PROTECTION OF CLASSIFIED INFORMATION

The National Security Office conducts security clearances for individuals and businesses, provides opinions on proposed individuals according to international treaties binding on the Slovak Republic, and maintains records related to the protection of classified information.

In addition to certificates and confirmations that allow access to national classified information, it ensures the issuance of security clearance certificates for individuals and industrial security certificates for businesses to handle classified information of NATO and the EU, and provides opinions on proposed individuals according to international treaties binding on the Slovak Republic.

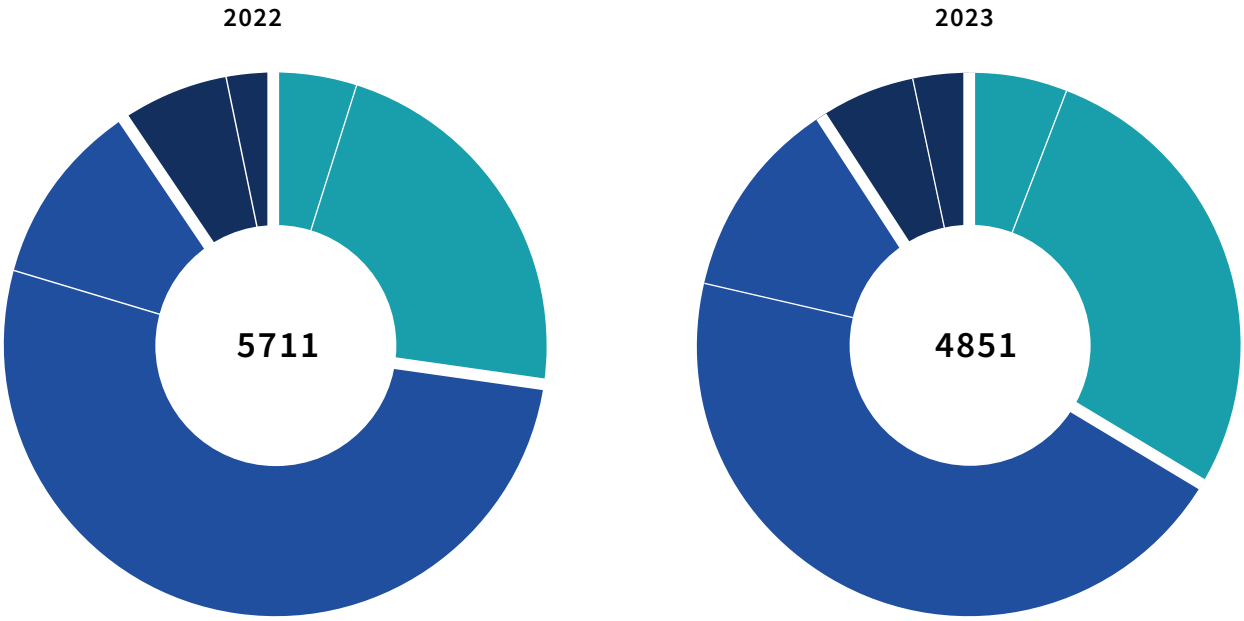


PERSONNEL SECURITY

The National Security Office issued **4,851 certificates** for handling classified information, **of which 2,757 were for the Ministry of Defense.**

Overview of certificates issued in 2022 and 2023

Classification Level	2022	2023
CONFIDENTIAL	**1570**	**1639**
For Ministry of Defense	279	290
SECRET	**3614**	**2771**
For Ministry of Defense	2985	2181
TOP SECRET	**527**	**441**
For Ministry of Defense	355	286
Total	**5711**	**4851**



The NBÚ issued 31 decisions. Individuals filed 13 appeals against the office's decisions. In two appeals, the office decided by self-remedy. The Committee of the National Council of the Slovak Republic for reviewing decisions of the National Security Office ruled on 13 appeals, rejected seven appeals, annulled two office decisions on appeal, and annulled two decisions following a ruling by the Supreme Administrative Court of the Slovak Republic. As of December 31, 2023, one appeal was still in the appeal process. One appeal was not accepted by the office.

No lawsuit was filed against the committee's decision at the Supreme Administrative Court. The Supreme Administrative Court ruled on a total of seven lawsuits in 2023 –

it rejected three lawsuits, annulled two committee decisions along with the office's decision, and annulled two office decisions.

Two constitutional complaints were filed with the Constitutional Court of the Slovak Republic. The Constitutional Court rejected one complaint.

Decisions of the office, appeals by individuals against office decisions, and lawsuits in 2022 and 2023

	2022	2023
OFFICE DECISIONS	**47**	**31**
APPEALS	**16**	**13**
Appeals – self-remedy (OA)	2	2
Appeals rejected by the committee (OZ)	15	7
Decisions annulled by the committee (RZ)	3	4
Lawsuits filed at the Supreme Court (NS)	6	0

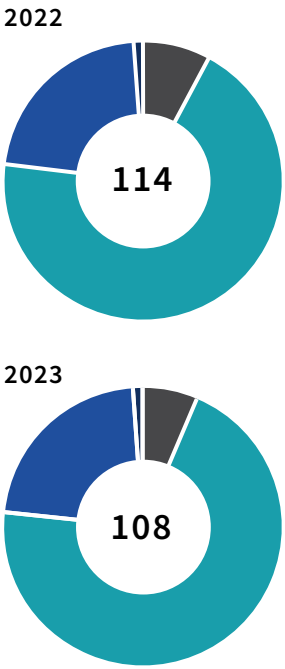
In 2023, **8,699 certificate**s were issued to proposed individuals – **of which 4,369 were NATO certificates and 4,330 were EU certificates.** Of the total number of NATO certificates, **the office issued 40 NATO ATOMAL certificates**, which authorize access to information on NATO's strategic nuclear deterrence and are issued to a limited circle of individuals.

INDUSTRIAL SECURITY

In 2023, the office issued 108 industrial security certificates – of which 7 were for the Restricted level, 76 for the Confidential level, 24 for the Secret level, and 1 for the Top Secret level.

Overview of industrial security certificates issued in 2022 and 2023

Classification Level	2022	2023
RESTRICTED	**9**	**7**
CONFIDENTIAL	**79**	**76**
SECRET	**25**	**24**
TOP SECRET	**1**	**1**
Total	**114**	**108**



In 2023, the office issued 12 decisions. Entrepreneurs filed four appeals against the office's decisions. The office did not decide on any appeal by self-remedy. The committee rejected one appeal and annulled one decision. As of December 31, 2023, two appeals were still in the appeal process.

No lawsuit was filed at the Supreme Administrative Court in 2023. The Supreme Administrative Court rejected one lawsuit and annulled one decision.

No complaint was filed with the Constitutional Court of the Slovak Republic.

Regarding classified information of NATO and the EU, in 2023, **16 NATO certificates and 14 EU certificates** were issued to entrepreneurs, authorizing them to handle NATO and/or EU classified information.

Decisions of the office, appeals by entrepreneurs against office decisions, and lawsuits in 2022 and 2023

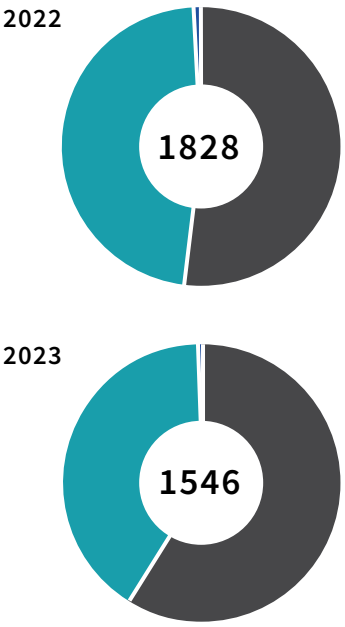
	2022	2023
OFFICE DECISIONS	**13**	**12**
APPEALS	**4**	**4**
Appeals – self-remedy	2	0
Appeals rejected by the committee (OZ)	2	1
Decisions annulled by the committee (RZ)	0	1
Lawsuits filed at the Supreme Court (NS)	0	0

EXCHANGE OF CLASSIFIED INFORMATION

In 2023, the office received and sent 1,546 classified pieces of information – internal distribution between departments is not included in this value. Since 2022, the electronic information system for records management has allowed the creation of classified information at the Restricted level, including its content.

Classification levels of classified information

Classification Level	2022	2023
RESTRICTED	**950**	**912**
CONFIDENTIAL	**867**	**631**
SECRET	**11**	**3**
TOP SECRET	**0**	**0**
Total	**1828**	**1546**



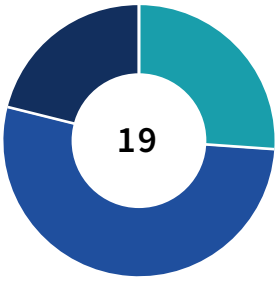
PHYSICAL AND OBJECT SECURITY

The NBÚ issued **43 certificates** for mechanical barriers and technical security devices.

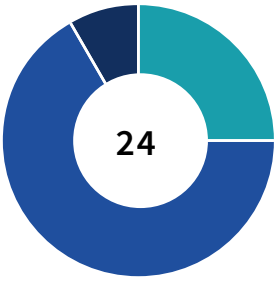
Classification levels of issued certificates

Classification Level	Mechanical Barriers (MZP)	Technical Security Devices (TZP)	MZP and TZP Total
RESTRICTED	0	0	0
CONFIDENTIAL	5	6	11
SECRET	10	16	26
TOP SECRET	4	2	6
Total	19	24	43

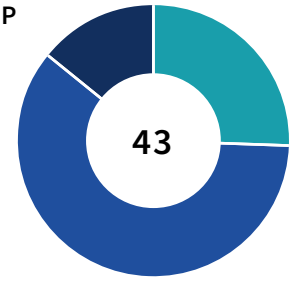
MZP



TZP



MZP a TZP

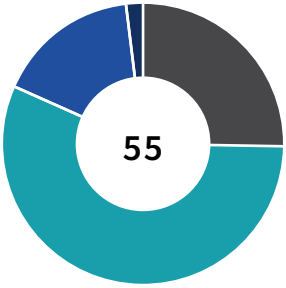


TECHNICAL SECURITY

The office issued **55 certificates** for technical devices and **23 amendments to issued technical device certificates**.

Classification levels of issued certificates

Classification Level	TS
RESTRICTED	14
CONFIDENTIAL	31
SECRET	9
TOP SECRET	1
Total	55



ACCREDITATION OF COMMUNICATION AND INFORMATION SYSTEMS

The National Security Office carried out 2 accreditations of communication and information systems: BICES SVK ELEMENT, SVK DEKMS in accordance with NATO Security Policy C-(2002)49-REV1, and 2 accreditations of communication and information systems: SVK EU DELEGATES PORTAL-R and SVK EU CORTESY in accordance with Council Decision (2013/488/EU).

PROTECTION AGAINST UNWANTED ELECTROMAGNETIC EMISSIONS

To ensure the protection of classified information from leakage through unwanted electromagnetic emissions, the office's personnel performed zonal measurements of protected spaces (using mobile measuring equipment).

During this period, no NEV measurements of technical devices (TP) and encryption protection tools (PŠOI) were conducted in the specialized TEMPEST laboratory due to the malfunctioning of measuring equipment in the TEMPEST laboratory.

The TEMPEST laboratory received 38 requests for measurements – based on these, technicians performed 92 zonal measurements of spaces and categorized 101 rooms.

Two requests for technical security inspections of spaces and motor vehicles were also received, based on which **14 room inspections and 18 service vehicle inspections were conducted.**

SECURITY AWARENESS

The spread of security awareness in the area of classified information protection is generally implemented through security personnel exams and professional training, in addition to the active external communication of the office. The office conducts exams and retraining through an online test via video.

In 2023, 486 candidates were invited to take the tests – 292 candidates passed the exam, 95 candidates failed, and the rest did not attend the exam.

A total of 139 candidates participated in retraining – 127 candidates successfully completed it, and the remaining number did not attend the exam.

At the request of the holder of the certificate of successful completion of the exam, four new certificates of completion of the exam (so-called "duplicates") were issued.

Based on the implementation protocol on mutual cooperation in conducting security personnel exams and retraining concluded between the Ministry of the Interior and the office, two inspections of compliance with this protocol were carried out.

Here is the translation of the text you provided: Lecturing activities are primarily carried out in cooperation with the Institute for Public Administration and are intended for both the public and private sectors. In 2023, the lectures were expanded to include the topic of the Act on the Protection of Classified Information.

The office also evaluates feedback from these events to adequately reflect the needs of the professional public.

ENCRYPTION PROTECTION OF INFORMATION

CERTIFICATION

The encryption protection system operates on the structure of departmental encryption authorities and their close cooperation with the office, which acts as the central encryption authority.

The main topics of mutual communication in 2023 included the certification of encryption protection tools, the issuance of amendments to the rules for using encryption protection tools, and questions regarding the recognition and adoption of foreign certificates.

The office issued 8 certificates for encryption protection tools.

Classification levels of issued certificates

Classification Level	TP
RESTRICTED	2
CONFIDENTIAL	2
SECRET	4
TOP SECRET	0
Total	8

2022

SECURED INFRASTRUCTURE

The office continued to distribute tools intended for the secure exchange of information between government institutions at the Restricted, Confidential, and Secret classification levels. The NBÚ ensured the protection of videoconferences and information transmission for government members.

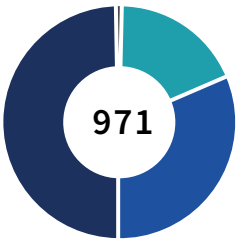
During the evaluation period, it was possible to increase the security and operational reliability of these systems through the use of new technologies for encryption protection tools. To maintain the achievement of set goals, we conducted personnel training focused on acquiring and developing professional skills for managing information systems, ensuring the protection of information systems, web services, technical devices, and encryption protection tools managed by the NBÚ.

In 2023, the office directly operated 6 systems with encryption protection within the secured infrastructure, operated or provided support for 482 endpoint devices, and provided services and support to 2,088 users. During the evaluation period, we recorded a total of 1,510 fulfilled requests from these users. At the same time, we continuously ensured the operational requirements of departments and provided support in the production and distribution of encryption material.

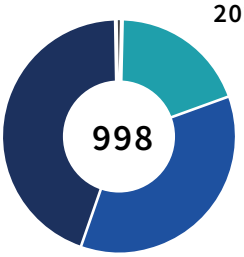
Secured Infrastructure

Classification Level	2021	2022	2023
SYSTEMS	5	6	6
ENDPOINT DEVICES	360	433	482
USER ACCOUNTS	621	805	2088
REQUESTS	971	998	1510

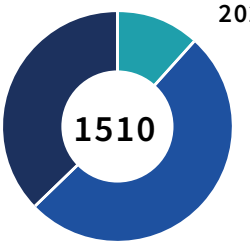
2021



2022



2023



TRUSTED SERVICES

The Council of the European Union adopted a common position on the proposal to revise Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trusted services for electronic transactions in the internal market (eIDAS).

The revision aims to provide universal access to secure and trustworthy electronic identification and authentication through the European Digital Identity Wallet on a mobile phone, through which a person can obtain their certification (electronic attestation of attributes) and send only the necessary data to the relying party (e.g., a car rental company).

The notification process, through which the relying party declares its intention to rely on the wallet, should be cost-effective, proportional to the risk, and ensure that the relying party provides at least the information necessary to authenticate access to the wallet. The Council proposes that the implementation period, set at 24 months, should start from the adoption of the implementing acts.

At the expert level, the office is preparing materials and actively participating in work defining procedures under Article 45d. In this case, Member States will ensure that measures are taken to enable qualified providers of electronic attestation of attributes, upon the user's request, to electronically verify the authenticity of these attributes.

The verification will be based on the relevant authentic source at the national level or through designated intermediaries recognized at the national level in accordance with national law or Union law, in cases where these attributes are based on authentic sources in the public sector.

Trusted Infrastructure

	2022	2023
CERTIFICATES	122 357	219 248

TRUSTED LIST

The office maintains and publishes on its website a trusted list containing information about qualified trusted service providers under the supervision of the Slovak Republic and information about the qualified trusted services provided.

In 2023, the office published trusted lists numbered 100 to 113.

LIST OF AUTHORIZATIONS

The list of authorizations, which serves as an information source for qualified trusted service providers issuing mandate certificates, is published by the office on its website.

In 2023, based on requests from state authorities and local government bodies, eight new authorizations were added to the list, and several existing authorizations were updated.

Throughout the year, the office published eight versions of the authorization list. Its current version was always supplemented with an archive of previous versions.

NEW TRUSTED SERVICES

The office received notifications from four qualified providers about their intention to provide a qualified trusted service.

A total of eight qualified statuses were granted for qualified trusted services. In 2023, five reports on conformity assessment conducted by the conformity assessment body were submitted to the supervisory authority by qualified trusted service providers within 24 months of the last audit, confirming that the qualified trusted service providers and the qualified trusted services they provide meet the requirements set out in Regulation (EU) No. 910/2014 of the European Parliament and of the Council.

The proceedings for granting two qualified statuses to one qualified trusted service provider were halted due to non-compliance with the regulation's requirements.

INTERNATIONAL STANDARDS DEVELOPMENT

In the development of international technical standards applicable for the implementation of the eIDAS regulation, an office member was part of expert groups of the European Commission, which analyze solutions and will form the basis for the preparation of implementing acts for the Digital Identity Wallet after the adoption of the eIDAS regulation revision.

CERTIFICATION

In 2023, the technical section did not receive any requests for certification of a secure product for qualified electronic signatures.

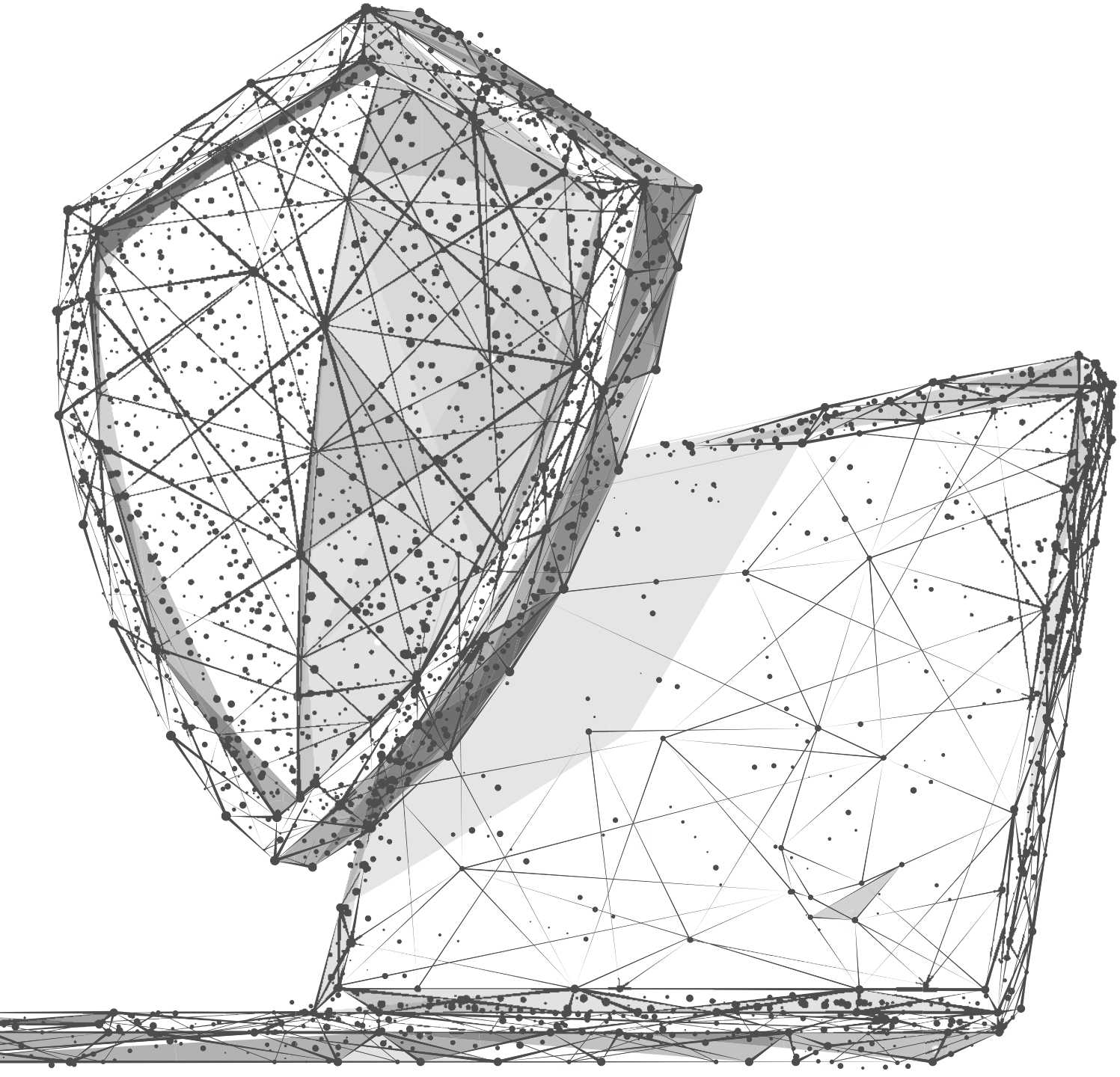
Qualified trusted service providers use devices for creating qualified electronic signatures or devices for creating qualified electronic seals already certified in another European Union country, which are listed in the list of devices certified by the European Union.

TRUSTED INFRASTRUCTURE

The office operates the Root Certification Authority of the Slovak Republic within the trusted infrastructure, which issues public key certificates and maintains a long-term database of issued qualified certificates with their validity status, issued by providers to whom the office has granted qualified status.

For the year 2023, a total of 219,248 certificates were recorded.

CYBERSECURITY



The National Security Authority, through the National Cybersecurity Center (NCKB SK-CERT), is developing its capabilities to ensure an open, secure, and protected national cyberspace. NCKB receives reports of cybersecurity incidents, analyzes them, evaluates them, monitors them, and coordinates their resolution.

It conducts security monitoring to collect information on cybersecurity incidents from various sources using specialized tools at the monitoring center. Additionally, it distributes warnings, thereby increasing the level of prevention.

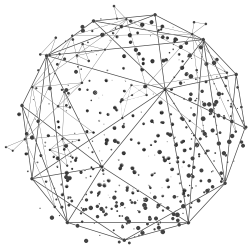
In 2023, NCKB's operational activities focused primarily on cybersecurity activities related to operators of essential services, including critical infrastructure elements. In addition to creating warnings, the office shared relevant information with partners based on international cooperation and its activities stemming from the analysis of reported and recorded incidents.

Number of Reported Cybersecurity Incidents in 2023

	Jan	Feb	Mar	Apr	Máj	Jún	Júl	Aug	Sep	Okt	Nov	Dec
Banking	6	17	10	7	6	6	4	6	3	1	8	3
Transportation	0	0	2	1	0	0	0	2	2	0	1	0
Digital Infrastructure	0	0	0	1	0	1	0	0	1	0	1	0
Electronic Communications	0	0	0	0	3	0	1	0	0	0	1	0
Energy	0	0	0	0	0	0	1	0	0	0	1	0
Financial Market Infrastructure	0	0	0	0	0	0	0	0	0	0	0	0
Postal Services	0	2	2	1	1	0	1	2	0	3	0	0
Industry	0	0	0	0	0	0	0	1	0	0	1	0
Water and Atmosphere	0	0	0	0	0	0	0	0	0	0	0	0
Public Administration	39	55	53	28	45	29	22	39	45	44	51	28
Healthcare	3	1	2	1	4	2	1	5	1	0	5	1
Others	34	38	36	23	29	28	24	31	18	35	39	25
Total	**82**	**113**	**105**	**62**	**88**	**66**	**54**	**86**	**70**	**83**	**108**	**57**

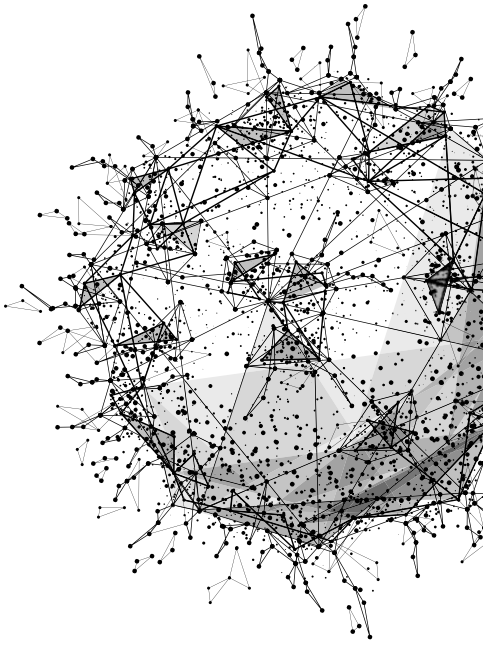
The National Security Authority recorded a total of **974 cybersecurity incident reports in 2023:**

- 19 reports of severe cybersecurity incidents (Level I)
- 4 reports of severe cybersecurity incidents (Level II)
- 3 reports of severe cybersecurity incidents (Level III)



The most common technical attack types were information gathering (611), denial of service (88), system intrusion (64), malicious code (49), and vulnerabilities (46).

Most of the reports came from voluntary reports, which outnumbered mandatory categorized reports. The most common reason for non-reporting was a lack of awareness of legal standards—entities were unaware they had a reporting obligation. With the upcoming amendment to the law in connection with NIS2, an increase in reports can be expected in the coming years—the amendment will extend the scope to additional entities.



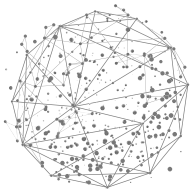
The highest number of incidents was reported in the public administration sector (478), banking (77), and healthcare (26). A higher number of reports suggests more incidents in the sector and may indicate a higher level of maturity of the reporting entity (not afraid to report, communicates, reports voluntary incidents, etc.).

In 2023, service disruption through DDoS attacks continued to be a popular method among attackers with varying degrees of knowledge and sophistication.

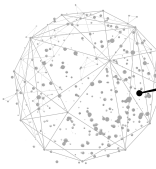
Ransomware was also on the rise. Compared to 2022, the number of ransomware attacks increased by 95%, affecting up to 72% of companies globally. The activity of professional gangs providing ransomware as a service (RaaS) continued to dominate this area. They improved their methods and tools, such as faster data encryption, obfuscation of traces, and more efficient data exfiltration.

The primary vector remained the leakage of login credentials directly into the infrastructure or VPN, their purchase, or retrieval from leaked databases. Attackers could also gain access through phishing, either by their activities or by purchasing services offered by other hacker groups that obtain login credentials for them.

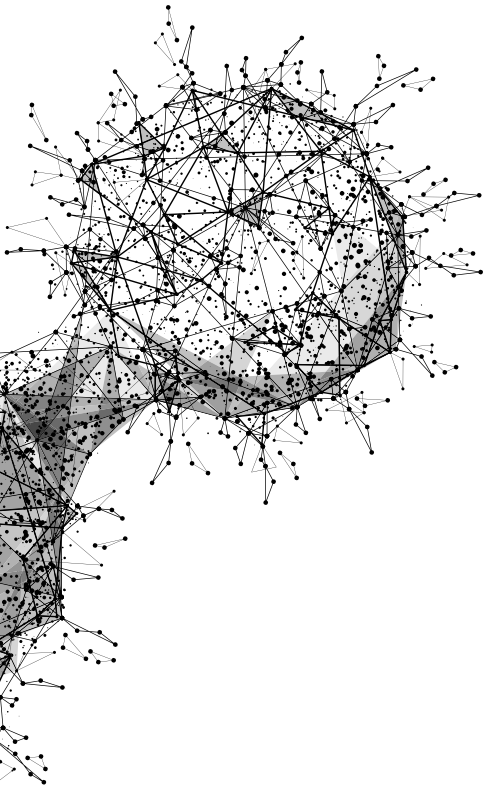
User-side deficiencies continued to be observed, such as misconfigurations and inadequate system security with insufficient cybersecurity hygiene. The highest number of exploited vulnerabilities was recorded in the media, recreation, and entertainment industries. These deficiencies appeared in the form of open remote access settings and other services to the internet, weak passwords, repeated use of the same passwords across different services, and unimplemented multi-factor authentication.



The rise in the popularity of artificial intelligence and the availability of language models, such as ChatGPT, Azure, or Grok, opened new doors for attackers and provided them with new tools to streamline their activities. They can generate higher-quality translations and texts for phishing emails and automate the generation of phishing emails in different languages. The increased sophistication of attacks was also due to the use of proprietary generative models, such as WormGPT, which do not contain security restrictions.



Regarding methods, attackers most commonly used redirect links to bypass email security mechanisms. The occurrence of vulnerable websites with open redirects has decreased. The use of URL shorteners to avoid detection mechanisms continues. The use of legitimate shorteners (e.g., bit.ly, cutt.ly) as well as shortening mechanisms of major social networks, such as X (Twitter) and LinkedIn, and a significant increase in the number of small URL shortening providers, added to the complexity of the situation.



Attackers' motivation for phishing activities can be divided into acquiring sensitive data, which is subsequently sold to third parties, and conducting phishing activities to spread malware, which can also serve to collect sensitive data.

Malvertising campaigns continued in 2023, spreading trojanized versions of frequently used software. The primary problem was people's tendency to automatically click on ads that have prominent positions in Google search results.

Phishing remains the most widespread and successful method of obtaining sensitive data and spreading malicious content. A common reason for system intrusion is email account compromise as a result of phishing, or through brute force attacks on unsecured login websites of mail servers, etc.

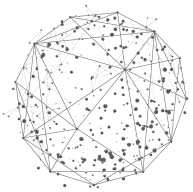
Phishing campaigns continued to be a popular method of acquiring sensitive data, as reflected in the significant increase in phishing amateurs. The increase was likely due to the ease of obtaining phishing tools developed and then sold or provided to attackers as a service (Phishing as a Service).

Impersonation in phishing remains prevalent, e.g., impersonation of banks, postal/delivery companies, or social networks. Activities that exploited geopolitically relevant events, such as the war in Ukraine or the war in Israel, were also observed.

Phishing campaigns continued to use social engineering to achieve their goals more effectively. The trends in obtaining sensitive information did not differ significantly from the previous year. The following phishing narratives prevailed:

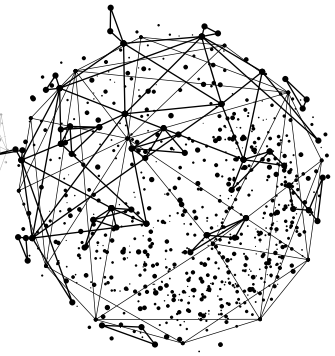
- Impersonation of delivery services
- Impersonation of network suppliers, banks, postal services
- Impersonation of the police and Interpol
- Impersonation of central government authorities, etc.
- Phishing and smishing were still carried out via SMS and email.

The phenomenon of sextortion and crypto scams (various services and pyramid schemes related to cryptocurrency investments) persists. Attackers gain the victim's trust by initially paying out commissions, but they stop at a certain point. This type of fraud has massive promotion—e.g., on social networks or organized physical meetings.



Another type of attack was whaling, which, despite its lower incidence, remains relevant. This attack can involve impersonating a company's CEO to request account status or payment.

The number of interactive forms of social engineering—often combined with phishing attacks—increased. Phishing websites now include interactive chats where the attacker guides the victim through various remote management services or navigates them during a phone call, pretending to be technical support.



In 2023, there were frequent DDoS attacks on critical infrastructure, the banking sector, and transportation (e.g., attacks on online parking systems and the websites of ZSSK, which disrupted online train ticket purchases, etc.). Several categorized incidents were also recorded.

A positive trend was the increased resilience of the infrastructure of victims after an attack, as well as in prevention (the high number of successful, widely reported attacks) and the influence of awareness raised by security forces (nationwide warnings, targeted/sector-specific warnings to organizations planned for attack by hacktivists). In most cases, the operation was restored after the attack ended.

In Slovakia, several devices infected with malware were identified, including SystemBC, IcedID, Ursnif, Trickbot, JS.Agent.USU, QuakBot, Qbot, Redline, Raccoon Stealer, Amadey, Lockbit 3.0. Noteworthy were media-reported cases from Matej Bel University, which was attacked by Medusalocker, and a campaign exploiting a VMware ESXi vulnerability.

The most common penetration vector in 2023 was phishing attacks. Inappropriate system configurations included open RDP, FTP, SSH, SMB, and ICS login interfaces with default settings and passwords/no login or poor password policies. Therefore, it is crucial to emphasize the need to follow security best practices, such as well-secured networks (e.g., using VPN, MFA, segmentation, minimizing threat surfaces—only essential services and devices should have internet access/connection).

The National Cybersecurity Center issued security recommendations and warnings against vulnerabilities and threats—52 comprehensive security bulletins and 428 security warnings. It alerted to 1,097 vulnerabilities and threats.

CYBERGAME

The National Security Authority organized the second edition of the cybersecurity competition called CyberGame.

The goal of the game was to bring the topic of cybersecurity closer to the public in an engaging and playful way and to raise awareness about threats and ways to protect their important data. The game also aimed to motivate people to get involved in cybersecurity and to identify talents in this field.

CyberGame ran from March 1 to May 10, 2023, and combined technical and non-technical tasks. Over 70 tasks were prepared in total. The game was divided into 6 branches—malware analysis, forensic analysis, cryptography, OSINT, hardening, and process and security management.

Each branch contained several scenarios (stories), which were added during the game's duration. Each scenario had several tasks logically linked. The game's principle was to collect points for so-called "flags." The player who collected the most points won.

A total of 2,333 players participated in the game. In 2023, the game was also opened to foreign players by creating an English version. From Slovakia, 1,788 players participated, and 545 users competed on the English platform. Players from 73 countries joined the game. There were 264 registered women, 67 teachers, 420 high school students, and 304 university students. The youngest registered player was 9 years old.

The winners of CyberGame received material prizes, and the best player, the second-best player, and the best female player in the women's category had the opportunity to visit a cybersecurity laboratory in Israel.

NATIONAL CYBERSECURITY CERTIFICATION AUTHORITY

The European Parliament and the Council (EU) adopted Regulation 2019/881 on the ENISA agency (European Union Agency for Cybersecurity) and on ICT cybersecurity certification, also known as the Cybersecurity Act. It also introduces an EU-wide framework for the certification of ICT products, services, and processes, aimed at increasing their trustworthiness.

Under Act No. 69/2018 on cybersecurity, the National Security Authority (NBÚ) is the national cybersecurity certification authority and the conformity assessment body (NCCA). It is responsible for developing the national cybersecurity strategy, managing and operating a unified cybersecurity information system, and issuing security standards, certification schemes, and procedures within the certification system.

The Slovak National Accreditation Service (SNAS) is the national accreditation body that accredits conformity assessment bodies. SNAS is authorized to perform accreditation by Act No. 53/2023 on the accreditation of conformity assessment bodies.

A conformity assessment body (CAB) is an entity that performs conformity assessment activities (certification, testing, etc.). CABs must be accredited for the specific activity. If a European cybersecurity certification scheme sets additional requirements for CABs, these must also be met by the CAB. The fulfillment of these additional requirements is confirmed by the issuance of authorization by the NCCA.

Currently, three cybersecurity schemes are being developed:

EUCC Scheme

The first scheme under the Cybersecurity Act is the proposal for the European cybersecurity certification scheme based on Common Criteria (CC). It is a globally recognized scheme applicable exclusively to ICT products. It includes “significant” and “high” assurance levels and does not allow for conformity self-assessment. The certificate is valid for five years and can be renewed.

EUCS Scheme

The second proposed European cybersecurity certification scheme is the scheme for cloud service (CS) certification. Unlike the EUCC scheme, it covers services and includes all three assurance levels—basic, significant, and high. However, it does not allow cloud service providers to perform conformity self-assessment.

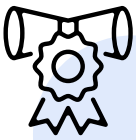
EU5G Scheme

The last proposed European cybersecurity certification scheme covers 5G networks. The proposal builds on the set of cybersecurity measures for 5G networks, and it is expected that the scheme will help mitigate additional risks associated with this ecosystem.

In 2023, the NBÚ successfully applied for a project aimed at strengthening testing and certification capacities in Slovakia, with the main goal of supporting the implementation of new European certification schemes into practice.

The project is divided into three stages. In the first stage, activities will focus on creating a legal framework for the introduction of schemes. In the second stage, activities will focus on supporting the accreditation of conformity assessment bodies for individual schemes. In the third stage, the focus will be on supporting the certification of products for manufacturers, service providers, or processes in ICT.

During the implementation phase, which is expected to last three years, we plan to support activities with a total amount of approximately 1 million euros. The project is fully funded by the EU through the Digital Europe program.



COMPETENCE AND CERTIFICATION CENTER FOR CYBERSECURITY

The state-funded organization, the Competence and Certification Center for Cybersecurity (KCCKB), serves as the National Coordination Center (NCC-SK) within the network of European coordination centers and the European Industrial, Technological, and Research Competence Center, as per Regulation (EU) No. 2021/887. Accreditation from the European Commission confirms the center's expertise and capacity to manage European financial funds for cybersecurity through directly managed EU programs.

In European financial programs, Slovakia achieved outstanding success at the EU level. In the Digital Europe program in 2023, Slovakia led among member states in the number of successful projects. The activities of the National Coordination Center significantly contributed to Slovak companies securing substantial financial resources to meet their cybersecurity needs.

In 2023, KCCKB, in collaboration with the NBÚ and the Ministry of Transport of the Slovak Republic, also concluded a grant agreement with the European Commission aimed at the effective implementation of the NIS2 directive in Slovakia. To continuously strengthen expert capacities, applications were submitted to the Ministry of Investment, Regional Development, and Informatization for additional funding of European projects from the Recovery and Resilience Plan.

A core goal of the Competence Center in 2023 was the intensive development of a professional community focused on cybersecurity. This effort led to the creation of strong partnerships, the sharing of best practices, and increased awareness of the importance of cybersecurity among businesses, academia, and the public sector. Several Slovak entities have already become members of the European cybersecurity community under Regulation (EU) No. 2021/887 through NCC-SK.

A significant part of the Competence Center's tasks is the performance of conformity assessments in cybersecurity, according to Regulation (EU) No. 2019/881 on the ENISA agency (European Union Agency for Cybersecurity) and the certification of cybersecurity for information and communication technologies (ICT) (Cybersecurity Act). Later, after its adoption, the Competence Center will also seek accreditation under the Cyber Resilience Act (CRA).

The Competence Center is currently accredited to certify cybersecurity auditors and managers under the specific regulation and the STN EN ISO/IEC 17024 standard, as well as integrated management systems for quality, information security, IT services, and business continuity management under the STN EN ISO/IEC 17021 standard.

The number of certified individuals increased in 2023 by 5 certified auditors and 7 certified managers.

In the 2022/806 legislative process, the Ministry of Justice accepted the National Security Authority's proposal to expand the list of expert fields to include a new field of cybersecurity. Based on this proposal, the Ministry of Justice of the Slovak Republic amended Decree No. 228/2018, which implements Act No. 382/2004 on Experts, Interpreters, and Translators. The Competence Center aims to be the first expert organization to perform expert activities in the new field of cybersecurity.

The Competence Center also succeeded in the field of adult education. In 2023, under Act No. 568/2009 on lifelong learning, it obtained accreditation from the Accreditation Commission of the Ministry of Education, Science, Research, and Sport of the Slovak Republic for further education programs for training Cybersecurity Managers and Cybersecurity Auditors. An updated educational scheme was also issued. The education portfolio was expanded to include a new specialized course and workshop on Continuity Management and a course on Information Security Management. Several existing course syllabi were updated.

In 2023, a total of 65 training sessions were conducted, including 8 courses on "Overview of Cybersecurity," 10 courses on "Cybersecurity Basics," 20 courses on "Cybersecurity Manager," 3 courses on "Cybersecurity Auditor," 9 specialized courses and workshops, 1 course on information security management according to ISO/IEC 27001:2022, and 14 free webinars aimed at raising cybersecurity awareness. A total of 1,033 participants attended these training activities during 2023.

The Competence Center organized a successful event focused on raising cybersecurity awareness called the "Cybersecurity Roadshow 2023." Several expert lectures were given at conferences and for students at selected universities in Slovakia.

The Competence Center issued a monthly leaflet to raise security awareness.

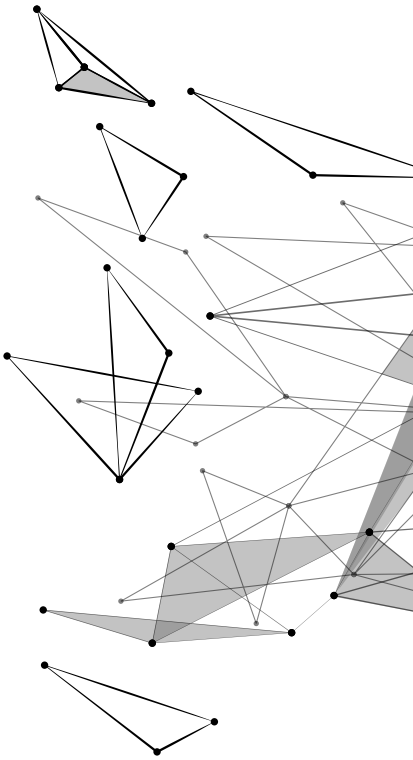
Every year, KCCKB conducts cybersecurity status surveys, which are then published as public documents. These include surveys among the general public and surveys conducted among small and medium-sized enterprises.

In 2023, the Competence Center continued to expand its network of organizations with which it established cooperation through memorandums of understanding.

In cooperation with NCKB SK-CERT, the Competence Center assembled a team of young people who represented Slovakia at the European CyberSecurity Challenge. This activity is overseen by the European Union Agency for Cybersecurity (ENISA). A total of 34 national teams participated—teams from 28 EU member states were joined by guest teams from the USA, Canada, Costa Rica, Serbia, Georgia, and the United Arab Emirates.

The competition took place from October 24 to 27 in Hamar, Norway. The Slovak team consisted of ten young talents—nine boys and one girl. The team prepared for several months, attending an international boot camp in Vienna in June and several boot camps in Bratislava under the guidance of technical coaches from SK-CERT.

INTERNATIONAL COOPERATION



Officials of the office develop relationships with foreign partners daily across dozens of organizations, platforms, and formats. In 2023, the NBÚ reaffirmed its commitment to building a security environment in line with the principles adopted in the European Union's Security Union Strategy for 2020-2025 and the European Union's Cybersecurity Strategy in the Digital Decade.

The priorities remain to increase the resilience of cybersecurity infrastructure, enhance cybersecurity, and establish processes to ensure security in both physical and digital environments.

EUROPEAN UNION

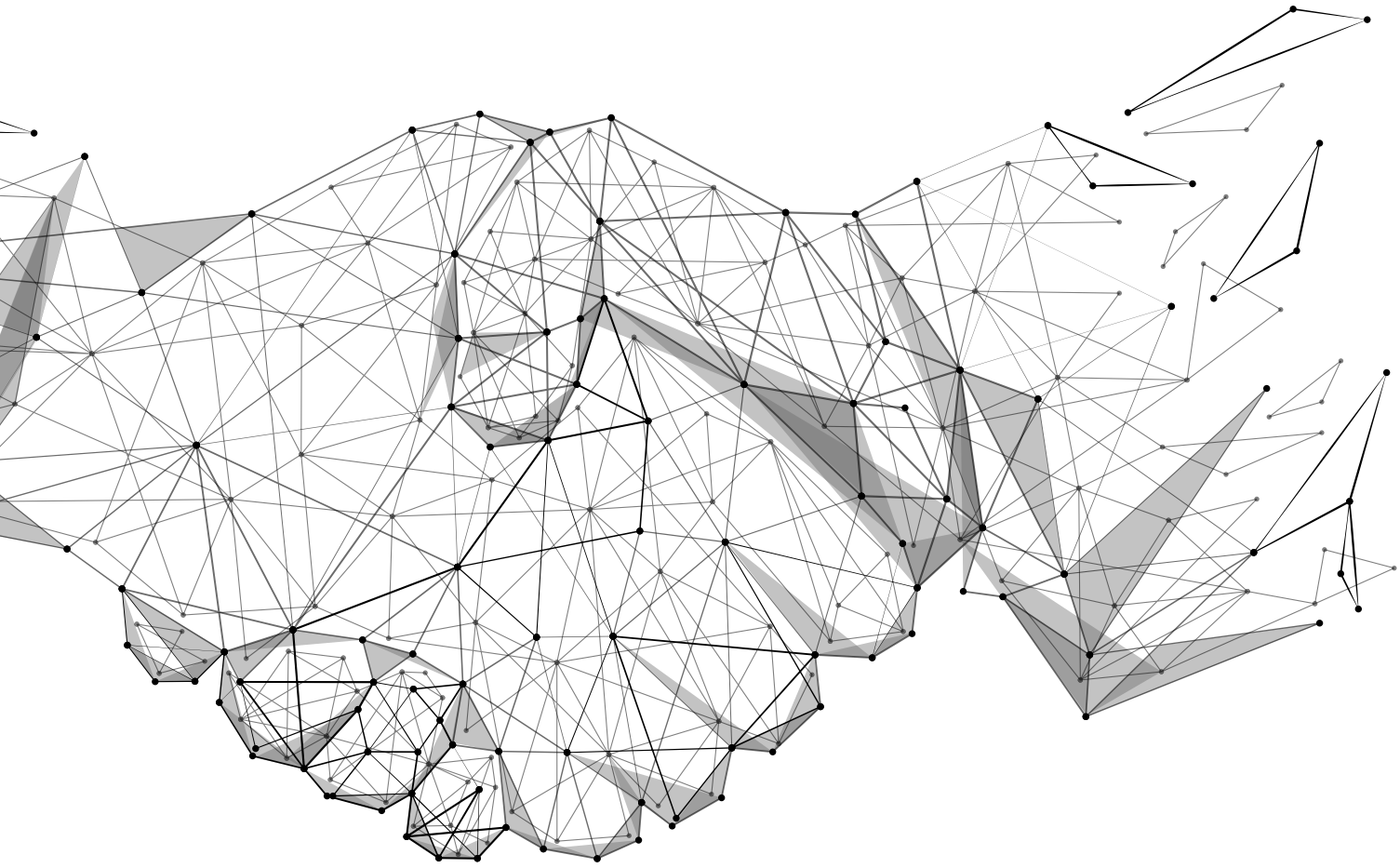
Our officials participated both in person and virtually in regular meetings of the EU Council Security Committee (CSC), the European Commission (EC) Expert Group on Security Policy (ComSEG), the European External Action Service (EEAS) Security Committee, the European Union Agency for the Space Programme (EUSPA) Security Committee, the TEMPEST Implementation Task Force (ITTF), and the European Union Agency for Cybersecurity (ENISA).

Within the EU Council, they revised security rules to address shortcomings identified in practice. In these working formats, the office actively engaged in the preparation of security standards to ensure the protection of classified information and the process of revising security rules.

The revision of the EU Council's security rules for the protection of EU[1] classified information (EUCI) continued, focusing on areas such as personnel and industrial security, security risk management, security assessments, violations of security rules, unauthorized handling of EUCI, and its sharing, as well as extraordinary or ad hoc access to EUCI.

The revision process was aimed at appendices containing specific measures in various areas of information security. At the end of 2023, the Council's Security Committee reviewed the draft regulation of the European Parliament (EP) and the Council on information security in the Union's institutions, bodies, offices, and agencies concerning unclassified information. Discussions also continued on the draft agreement between the EU and the USA, which establishes security procedures for launching Galileo satellites from U.S. territory.

1) Rozhodnutie Rady 2013/488/EÚ o bezpečnostných predpisoch na ochranu utajovaných skutočností EÚ



The year 2023 was exceptionally active in legislation within the European Council (the Council) and the European Parliament. During the Swedish and Spanish presidencies, three legal texts were finalized at the level of the Council's preparatory and political bodies, particularly in the Horizontal Working Group on Cyber Issues.

The first was the proposal for Regulation EP and Council 2023/2841, establishing measures to ensure a high common level of cybersecurity in the Union's institutions, bodies, offices, and agencies (EUIBAs).

The second was the proposal for a regulation of the EP and the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (CRA).

The last was the proposal for a regulation of the EP and the Council amending the eIDAS Regulation concerning the establishment of a framework for a European Digital Identity (eIDAS2). Publication in the Official Journal of the EU is expected in the first quarter of 2024.

Slovakia actively supported the goals of these legal texts. During the negotiations, it submitted many positively received comments and suggestions. The adoption of this legislation will strengthen the level of cybersecurity in European institutions, increase consumer protection when purchasing and using various software and hardware products with digital elements, and create a framework for simple, EU-wide identity verification for citizens using electronic services.

In April 2023, the European Commission published a cybersecurity package consisting of two new legislative and one non-legislative documents.

These included a proposal for a regulation of the EP and the Council establishing measures to strengthen solidarity and capacities in the Union for detecting cyber threats and incidents, preparing for and responding to them (CySOLa), a proposal for a regulation of the EP and the Council amending Regulation (EU) 2019/881 concerning managed security services (CSA+), and a communication on the creation of a Cybersecurity Skills Academy.

Considering the need for rapid progress to achieve a political agreement before the end of the legislative cycle in early 2024, the Horizontal Working Group on Cyber Issues engaged in intensive discussions on these documents.

The Committee of Permanent Representatives was thus able to give the presidency a mandate for final discussions with the EP and EC on CSA+ and CySOLa. A political agreement on both documents is expected in the first quarter of 2024. It is worth noting that while the Slovak Republic supported the main ideas and goals of the solidarity proposal, provided it was significantly revised—which it was—it abstained from voting on the CSA+ proposal, which it considered duplicative of existing legislation.

It is also worth adding that at the level of comitology committees, under already adopted EU secondary legislation—especially the revised Directive on measures to ensure a high common level of cybersecurity in the Union (NIS2 Directive), the Cybersecurity Act (CSA), or other relevant legislation—the office participated in technical discussions on implementing various measures.

Particular attention deserves the preparation of candidate cybersecurity schemes EUCC (Common Criteria) and EUCS (Cloud Schemes), which are expected to be published in the Official Journal of the EU in the first quarter of 2024.

The Horizontal Working Group on Cyber Issues (HWPCI), in its non-legislative activities, also focused on other strategic elements in the area of cyber diplomacy. In 2023, it succeeded in updating the Cyber Diplomatic Toolbox framework, enabling the Council to adopt more effective responses to malicious cyber activities, including sanctions.

This framework included expanded implementation guidelines that took into account the ongoing conflict in Ukraine, the impact of new technologies, and the deteriorating geopolitical security situation. Additionally, in May 2023, the Council, based on HWPCI's work, adopted conclusions on European cyber defense policy, and in June 2023, conclusions on digital diplomacy. The NBÚ participated in the creation and balancing of these strategic documents.

Representatives of the office also attended meetings of the European Union Cybersecurity Certification Group (ECCG). The main topic was the preparation of the final version of the EC regulation concerning the implementation of the horizontal cybersecurity certification scheme for products and protective documents, adding

references to existing national schemes, and agreeing that mutual recognition between member states should be full.

Officials from the office and the National Cyber Security Center SK-CERT participated in EC working formats such as the Cooperation Group – NIS and the Working Group on the Assessment of National Strategies. Their main task was to ensure and intensify strategic and analytical cooperation and information sharing between the cybersecurity authorities of member states and their units.

Key priorities of the Cooperation Group – NIS included preparing for the implementation of Directive (EU) 2022/2555 of the European Parliament and the Council of December 14, 2022, on measures to ensure a high common level of security of networks and information systems in the European Union, which amends Regulation (EU) No. 910/2014 and Directive (EU) 2018/1972 and repeals Directive (EU) 2016/1148 (NIS2 Directive), and the related application of new tools.

In addition to addressing the national implementation of the NIS2 Directive, topics related to risk assessment and risk scenarios, as well as the conclusions of the Council on the evolution of the EU's approach to cybersecurity, were also added.

New sub-platforms were created in the Cooperation Group, such as the Work Stream on Risk Evaluation, the Work Stream on Supervision, and the Work Stream WHOIS, aimed at addressing risk assessment, oversight, control, and support for security and internet stability.

In the second half of the year, the Cooperation Group – NIS, due to incidents in the Baltic Sea, also focused on discussing underwater infrastructure (data cables, pipelines, and their landing points).

Simultaneously, there was significant development in the relationship between the Cooperation Group and the Critical Infrastructure Resilience Building Group—both platforms met for the first time.

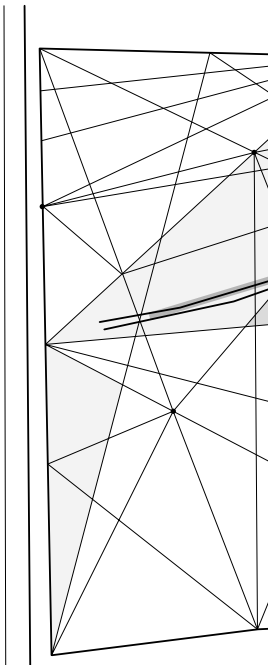
ENISA developed a roadmap for cybersecurity exercise needs. States shared their experiences with the most serious cybersecurity incidents and threats they faced during the year (ransomware dominated again). Additionally, ENISA prepared a presentation focused on its new obligations, particularly those related to member states' notification requirements. The NBÚ also participated in the following Work Stream cooperation groups:

- Work Stream – Group focused on notification obligations of essential service operators
- Work Stream – Group for managing large-scale cybersecurity incidents
- Work Stream – Group for digital infrastructure
- Work Stream 5G – Group for securing and protecting 5G networks
- Work Stream – Group for the healthcare sector
- Work Stream – Group for elections

The EU CyberNet stakeholder community, which brings together national authorities and institutions operating in cybersecurity, expert groups in this field, think tanks, and academic institutions based in EU member states, also continued its development.

EU CyberNet organized numerous workshops and conferences throughout the year, focusing on current cybersecurity topics, where office officials enhanced their expertise and expanded their knowledge by participating in these activities.

Regular meetings of the European External Action Service (EEAS) Security Committee (SC EEAS) brought about the revision and implementation of the security awareness program and intensified staff training on potential cyber risks.



SC EEAS also finalized work on a handbook to assist not only newcomers in handling EU classified information (EUCI). It continued revising guidelines for the creation and handling of EUCI and the contingency plan for the evacuation and destruction of EUCI. SC EEAS staff contributed to building resilience and security awareness among EU foreign delegations through training, workshops, and support programs.

In November, an international conference of European Partners Against Corruption and the European Contact-Point Network Against Corruption (EPAC/EACN) was held in Dublin, Ireland. The conference focused on strengthening international cooperation and exchanging information on corruption prevention and police oversight, as well as on procedures for asset recovery from criminal activities.

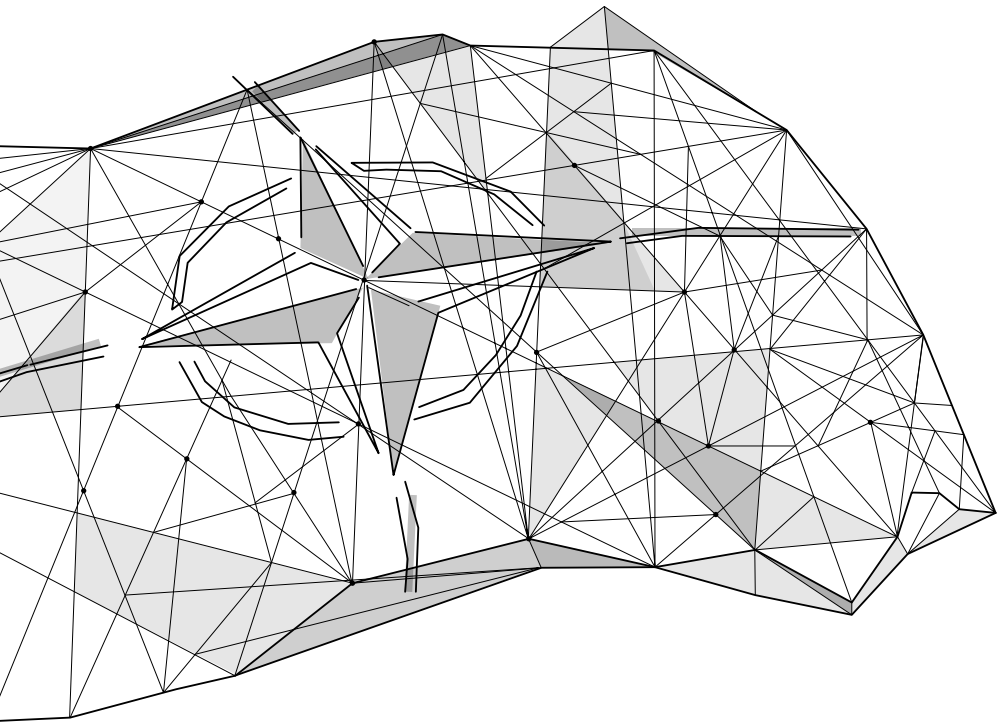
The most significant benefit of the event was the establishment of communication, expert discussions, and the personal exchange of knowledge and practical methods in preventing, detecting, and investigating corruption-related crimes. It also facilitated the sharing of experiences among the member units of EPAC/EACN and improved operational cooperation between anti-corruption and inspection agencies within the international EPAC/EACN network.

Additionally, activities and efforts related to the institutionalization of the European Cybersecurity Competence Centre (ECCC) and the network of National Coordination Centres continued. The main role of this centre is to serve the EU's strategic interest in maintaining and developing cybersecurity capacities to ensure a unified digital market, protect critical networks and information systems, and provide essential services in this area. The KCCKB actively represented the office on the ECCC's governing board while also fulfilling its role as a national coordination centre.

A highly positive development was the nomination of a candidate from Slovakia for the vacant position of Executive Director of the ECCC, a role that will be selected by the European Commission and appointed by the governing board.

In 2023, office representatives participated in regular meetings of the EU Space Programme Security Committee at the European Union Agency for the Space Programme (EUSPA). The primary topic of discussion in the EUSPA's main Security Committee was the development of General Security Requirements (GSR) and the establishment of a framework for determining the classification levels for various components of EU space programs.

These extensive documents were prepared within various supporting working groups, such as the Working Group on the Security of the Galileo Program, GOVSATCOM, Copernicus, or Egnos. In connection with the GOVSATCOM program, new working groups under the EUSPA Security Committee were established, including the Working Group on Security for EuroQCI (Quantum Communication Infrastructure). This group is involved in discussions on the cross-cutting theme of quantum communication infrastructure, which is to be used in connection with the GOVSATCOM program and will ensure a high level of encryption, resilience, and thus security—the network is also expected to be adapted for the transmission of classified information.



NATO

The NATO Security Committee (SC) convened in all its formats, covering security policies, communication and information systems security, and meetings at the level of security office directors.

In 2023, extensive revisions of NATO's security rules continued, with a particular focus on supporting documents related to NATO's primary security policy, C-M(2002)49-REV1. A key topic of discussion was the Directive on Industrial Security and Classified Contracts. The committee established a working group of experts from member states to prepare a revised Directive on Security Projects and Industrial Security.

A new working group composed of members from the NATO Archives Committee and the SC was formed to address the issue of mass declassification of NATO classified information. Additionally, NATO is revising its fundamental guidelines and supporting documents for security policies, including guidelines on personnel, physical, facility, and administrative security, as well as the protection of NATO classified information at the Restricted level.

In May, the NATO Archives Committee (AC) held a session to introduce a new initiative for procedures to mass declassify documents from the Yugoslav war era. Meetings between representatives of NATO AC and SC in the security policy format are planned to advance this goal.

During the October session at the highest level (Principals), participants were presented with the 2024 program, which was expanded to include two new supporting documents. The first will address telework, and the second will cover foreign ownership, control, and influence (FOCI) over companies participating in NATO contracts.

A significant milestone in cybersecurity and defense was the July summit in Vilnius, where the pilot mechanism for the Virtual Cyber Incident Support Capability (VCISC) was tested. VCISC is a virtual capability that allies can use if they are unable to address

the consequences of malicious cyber activity on their own. Member states can request assistance through NATO.

Before the summit, Slovakia became a voluntary contributor to VCISC, and representatives from the office actively participated in its pilot testing. Lessons learned from the exercise will be incorporated into setting goals for the mechanism and building the VCISC community.

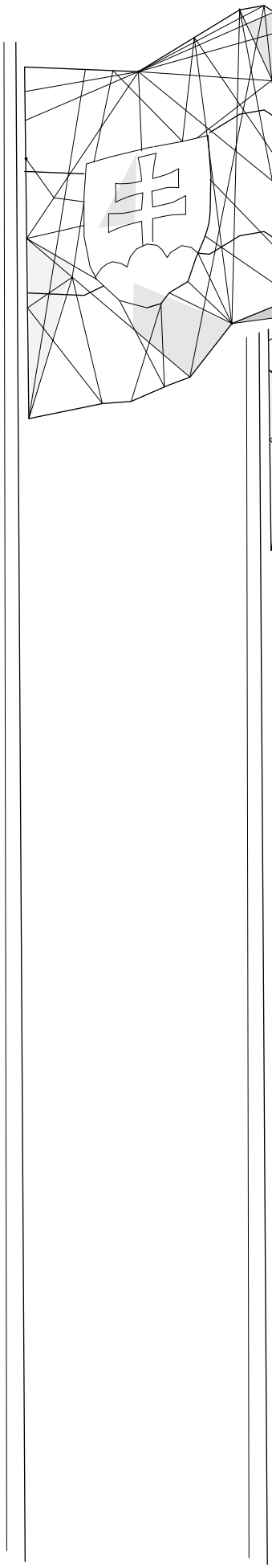
In November, Berlin hosted the first annual NATO Cyber Defense Conference, bringing together all three levels of NATO structures and representatives from the 31 allies. Slovakia was represented at the political, technical, and military levels by officials from the Ministry of Foreign and European Affairs of the Slovak Republic, the National Security Authority (NBÚ), and the Cyber Defense Center.

The conference's main messages emphasized the necessity of cooperation across all levels with the private sector, the need to build common situational awareness, timely information sharing for rapid response to malicious cyber activities, partnership building and cooperation (primarily with the EU), keeping pace with the implementation of new technologies, greater proactivity, and potential joint attribution.

On a bilateral level, office representatives held talks with NATO officials in two areas. Representatives from the NOS security clearance department sought details on the security clearance process and the issuance of certificates, as these details were needed for the preparation of the NATO Personnel Security Handbook, which clearly explains the procedures for obtaining a certificate for individuals working within NATO structures.

In the summer of 2023, our representatives visited NATO headquarters in Brussels, where they were briefed on physical and facility security details. The knowledge gained will be used in the project to enhance physical and facility security at the office.

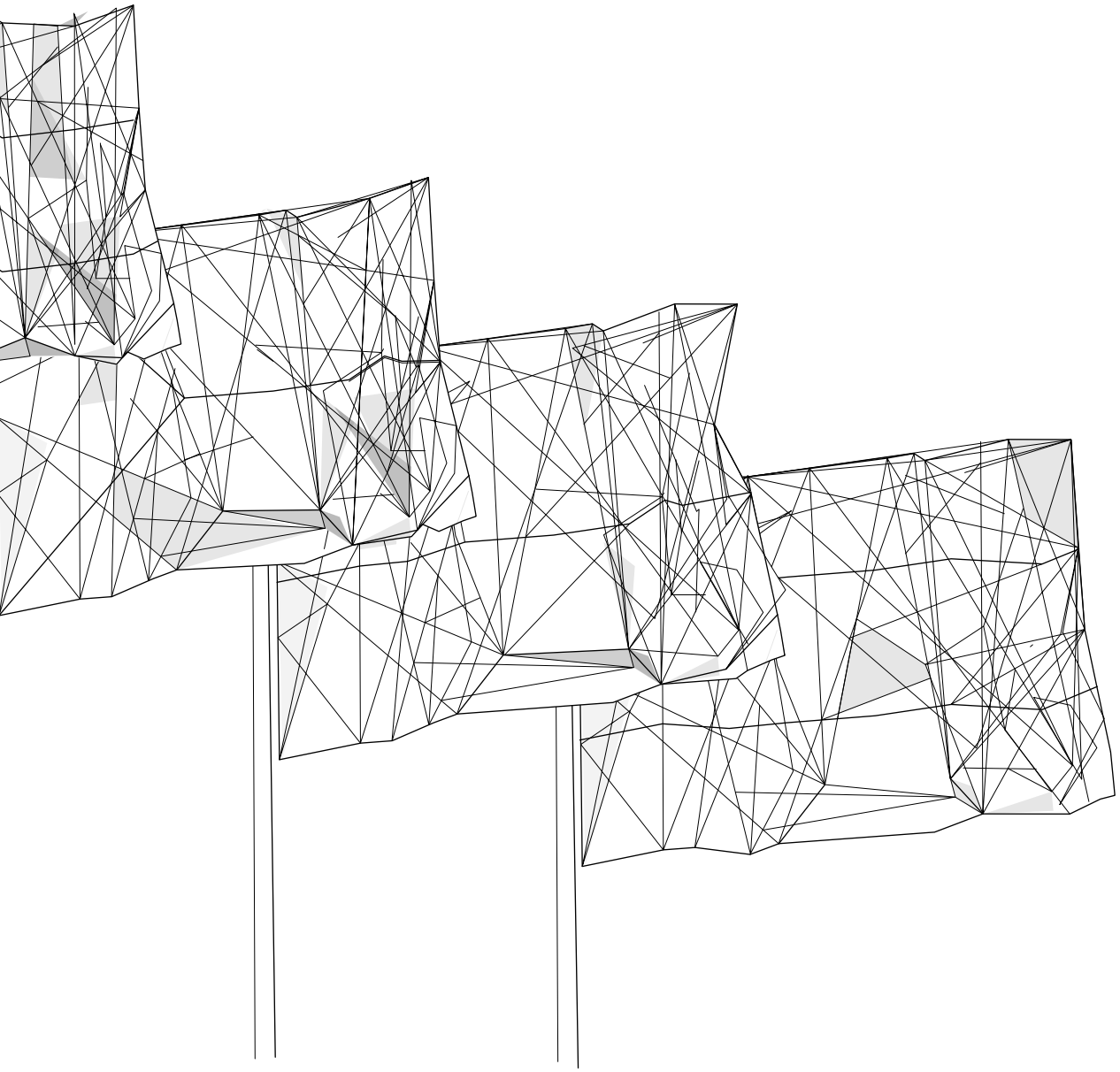
The office also participated in the joint NATO exercise Able Staff 2023 in November 2023, which aimed to test communication procedures related to nuclear planning, practice applicable measures of the alliance's crisis response system, enhance consultation capabilities, and provide practical training for personnel at NATO headquarters, SHAPE (Supreme Headquarters Allied Powers Europe), and national command centers.



REGIONAL COOPERATION

In 2023, the Central European Cybersecurity Platform was chaired by the Czech NÚKIB. Office representatives participated in platform discussions with colleagues from Hungary, Poland, and Austria.

The discussions focused on current EU-level topics, mutual intersections, and experiences in these areas. Representatives from various countries discussed the transposition of NIS2, research, development, and regional cooperation, where the Czech side presented its approach to cybersecurity exercises and the roles of legal advisors.



INTERNATIONAL ACTIVITIES

In September 2023, the 37th plenary session of the Multinational Industrial Security Working Group (MISWG) was held. This working group is a recognized body for cooperation in best practices in international industrial security, with nearly 40 countries, including Slovakia, represented.

The main goal of the meeting was to support, improve, and harmonize common international best practices for protecting classified information (in the field of industrial security) and other forms of government-controlled information that face current and new security threats and challenges in this area.

During the meeting, office representatives engaged in several bilateral discussions to deepen cooperation with partners in the areas of classified information protection and cybersecurity, including the Netherlands, Italy, Denmark, Japan, Luxembourg, Spain, Hungary, Romania, Australia, and Macedonia.

Representatives from the office also worked within the CCRA—Common Criteria Recognition Arrangement Group.

BILATERAL RELATIONS

The National Cybersecurity Centre regularly exchanged information on current national-level legislation, vulnerabilities, threats, and incidents, and shared information on best practices with its international partners outside the EU.

In March 2023, the government approved an international treaty with the European Space Agency on the exchange and mutual protection of classified information.

Negotiations for a classified information protection treaty with the Netherlands began in the spring and continued with inter-ministerial review in the fall.

Throughout the year, Director Roman Konečný met with Czech partners from GIBS, NBÚ (Czech Republic), and NÚKIB. A memorandum of cooperation was also signed with the last-mentioned institution. Both organizations confirmed active and long-term cooperation on security issues. Our colleagues also met with experts from NÚKIB during the innovation of the national TEMPEST laboratory for testing and skill development with new measuring equipment.

In return, we welcomed Czech NBÚ officials to our office to discuss the harmonization of procedures for recognizing security clearances. Both offices then published relevant methodologies on their websites. In June, representatives of the central registries of both countries met reciprocally.

Office representatives also participated in discussions on a proposed treaty between the government and the Organization for Joint Armament Cooperation (OCCAR). The agreement will allow Slovak entities to participate in European defense industry projects.

In March and August, we welcomed representatives from Indonesia. The aim was to further deepen cooperation in security, regional security challenges, and the development of security cooperation between Indonesia and the Slovak Republic.

The main point was the signing of a Memorandum of Understanding between both parties (March 2023). The memorandum identified 17 areas of cooperation, including the protection against active cyber threats, support for responsible state behavior in cyberspace, cyber threat intelligence (CTI), and strategic analysis; security of the information and communication technology supply chain; capacity building, and more.

In November, the NBÚ hosted its first delegation from the African continent—Kenya. The delegation mainly consisted of representatives from security sectors and cybersecurity specialists. The Kenyan side expressed interest in closer cooperation. The meeting's agenda focused on cybersecurity issues.

Throughout the year, short meetings also sparked interest in establishing cooperation with the Taipei Representative Office in Bratislava, the Permanent Commission of the Czech Senate for Media, the Permanent Representation of the Kingdom of Belgium to the UN in Vienna, and France regarding cooperation in the development and implementation of a European cybersecurity scheme for cloud services.

In September 2023, a liaison officer position was established at the Slovak Republic's Embassy in Washington D.C. The primary task of this role is to create close cooperation in cybersecurity and develop collaboration with the relevant U.S. agencies dealing with the protection of classified information.

EXCHANGE OF FOREIGN INFORMATION

The digitalization of foreign classified information registers through online connections with classified information registers of public authorities enables secure, faster, and more flexible recording and electronic distribution of classified information.

Last year, the NBÚ continued to provide methodological assistance to individual classified information registers in the electronic recording of classified information.

The central register processed 3,716 NATO classified items and 2,999 EU classified items. The office also facilitated the exchange of 172 classified items from foreign powers.

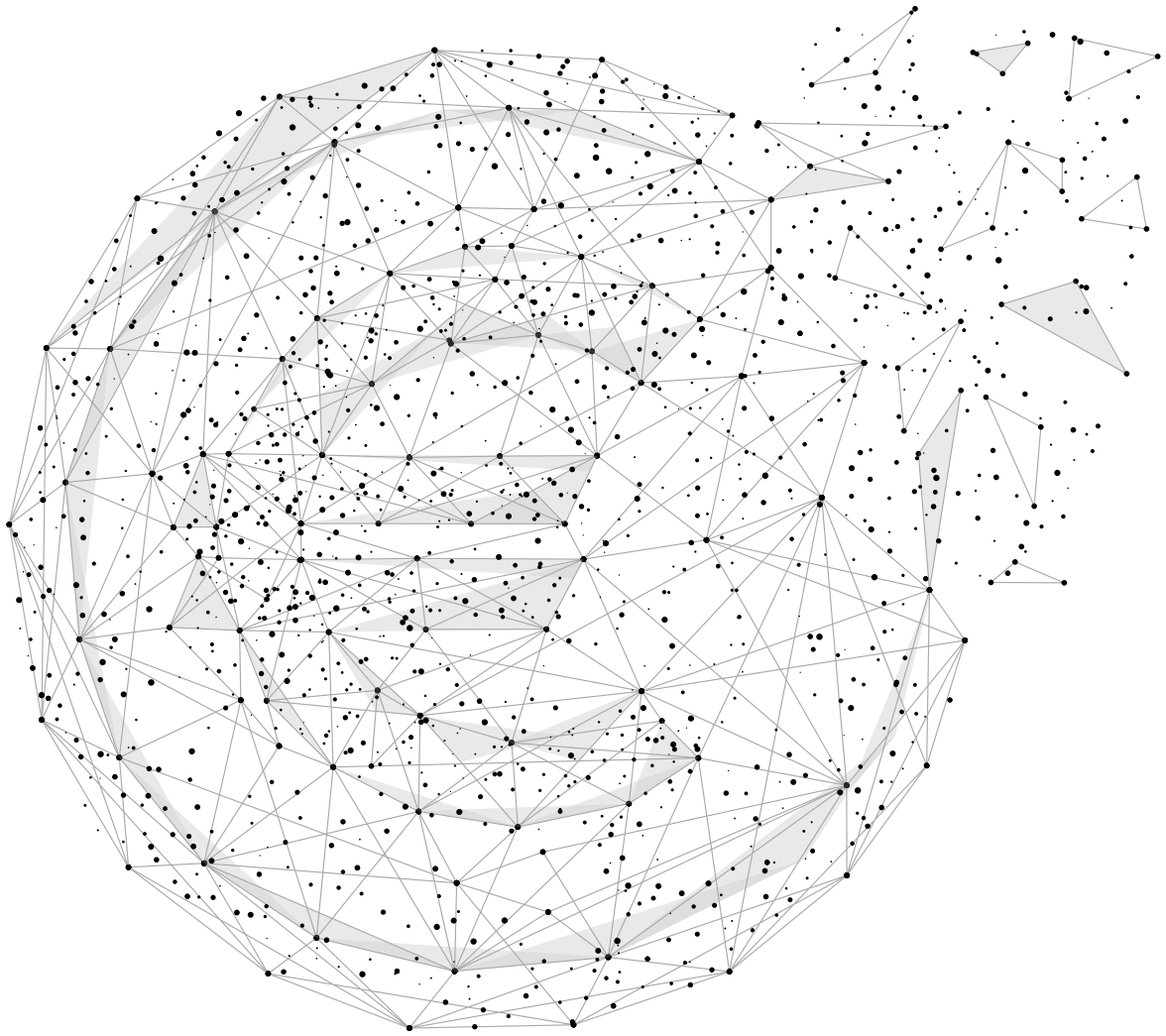
Since 2010, the NATO ATOMAL classified information register has been operational at the office; however, no classified documents were registered in it last year.

Level of Classification	2022	2023
NATO — RESTRICTED	1833	1863
EU — RESTRICTED	886	1115
FOREIGN POWER — RESTRICTED	114	87
NATO — CONFIDENTIAL	565	732
EU — CONFIDENTIAL	750	1117
FOREIGN POWER — CONFIDENTIAL	39	59
NATO — SECRET	1770	1121
EU — SECRET	886	767
FOREIGN POWER — SECRET	7	26
NATO — TOP SECRET	0	0
EU — TOP SECRET	0	0
FOREIGN POWER — TOP SECRET	0	0
NATO – Total	**4168**	**3716**
EU — Total	**2522**	**2999**
FOREIGN POWER — Total	**160**	**172**

The National Security Authority has maintained a central repository for classified information since 2021, intended for the temporary storage of classified materials with permanent documentary value. This repository is located at a branch office in Topoľčianky.

Budget Management

The breakdown of binding budget indicators for Chapter 41 – National Security Authority for 2023, the impact of budgetary measures on the adjusted budget, actual expenditure as of December 31, 2023, and the percentage assessment of fulfillment against the adjusted budget is as follows:



The binding budget indicators for 2023, as approved by Act No. 526/2022 Coll. on the state budget for 2023 dated December 22, 2022, and its subsequent amendments, were adhered to by the Authority. The Authority managed financial resources in accordance with the principles of economy, efficiency, and effectiveness, while ensuring compliance with legislative regulations, particularly Act No. 523/2004 Coll. on the budgetary rules of public administration, Act No. 357/2015 Coll. on financial control and audit, Act No. 343/2015 Coll. on public procurement, resolutions of the Government of the Slovak Republic, and methodological guidelines and instructions from the Ministry of Finance of the Slovak Republic.

Table 1: National Security Authority Budget for 2023 (in euros)

CATEGORY	APPROVED BUDGET	ADJUSTED BUDGET	ACTUAL AS OF 31.12.2023	PLNENIE K UPR. ROZPOČTU
I. Chapter Revenues	**20 000,00**	**20 000,00**	**32 680,43**	**163,40%**
A. Binding Indicator	20 000,00	20 000,00	32 680,43	163,40%
B. European Union Funds	0,00	0,00	0,00	
II. Total Chapter Expenditures	**14 612 255,00**	**19 658 606,55**	**19 423 072,86**	**98,80%**
A. Expenditures without funds per §17(4) of Act No. 523/2004 Coll. and EU funds	**14 610 255,00**	**19 645 859,10**	**19 410 325,41**	**98,80%**
of which:				
A.1. Budgetary Chapter Resources	14 610 255,00	15 296 338,21	15 085 854,44	98,62%
z toho: kód zdroja 111 + 11H + 11UA	14 610 255,00	15 115 288,21	14 906 166,52	98,65%
kód zdroja 131	0,00	181 050,00	179 687,92	99,25%
A.2. Co-financing funds	0,00	1 099 972,83	1 087 357,54	98,85%
z toho: kód zdroja 1AC2	0,00	52 746,43	52 746,43	100,00%
kód zdroja 1AC3	0,00	78 985,66	77 117,32	97,63%
kód zdroja 3AA2	0,00	520 703,24	514 923,71	98,89%
kód zdroja 3AA3	0,00	447 537,50	442 570,08	98,89%
A.3. Salaries, Wages, Service Income, and Other Personal Settlements | 254 persons | 254 persons | 223 persons*	7 542 875,00	7 723 430,64	7 608 964,94	98,52%
toho: mzdy, platy, služ. príjmy a ost. os. vyrovnania aparátu ústred.				
orgánu (kód zdroja 111 + 11H + 11UA)	7 542 875,00	7 723 430,64	7 608 964,94	98,52%
Počet zamestnancov RO podľa prílohy č. 1 k uzneseniu vlády SR č. 577/2021	254 osôb	254 osôb	223 osôb*	87,80%
z toho: aparát ústredného orgánu	254 osôb	254 osôb	223 osôb*	87,80%
administratívne kapacity rozp. organizácií osobitne sledované podľa prílohy č. 1 k uzneseniu vlády SR č. 636/2022	0 osôb	0 osôb	0 osôb	
z toho: aparát ústredného orgánu	0 osôb	0 osôb	0 osôb	
A.4. Capital Expenditures (without co-financing funds)	500 000,00	4 661 852,53	4 655 911,94	99,87%
z toho: kód zdroja 111	500 000,00	739 552,40	734 973,89	99,38%
kód zdroja 131L	0,00	181 050,00	179 687,92	99,25%
kód zdroja 1AA1	0,00	1 414 883,84	1 414 883,84	100,00%
kód zdroja 3AA1	0,00	1 402 015,62	1 402 015,62	100,00%
kód zdroja 3AA2	0,00	497 099,91	497 099,91	100,00%
kód zdroja 3AA3	0,00	427 250,76	427 250,76	100,00%
A.5. Recovery Plan and Resilience Funds for VAT Payment	0,00	0,00	0,00	0,00
B. B. Funds per §17(4) of Act No. 523/2004 Coll. (Podľa § 17 ods. 4 z. č. 523/2004 Z. z. je RO oprávnená čerpať tento limit do výšky rozpočt. príjmov skut. prijatých a je oprávnená prekročiť limit výdavkov z dôvodu dosiahnutia vyšších ako rozpočt. príjmov.)	**2 000,00**	**12 747,45**	**12 747,45**	**100,00%**
C. C. European Union Funds	**0,00**	**3 249 548,06**	**3 237 113,43**	**99,62%**
z toho: kód zdroja 3AA1	0,00	1 486 507,24	1 486 507,24	100,00%
kód zdroja 1AC1	0,00	298 896,42	298 896,42	100,00%
kód zdroja 3AA1	0,00	1 464 144,40	1 451 709,77	99,15%
C.1 Recovery Plan and Resilience Funds	**0,00**	**0,00**	**0,00**	
D. State Budget Expenditures for SR Government Programs	**14 612 255,00**	**19 658 606,55**	**19 423 072,86**	**98,80%**
0D9 Bezpečnosť informácií	14 477 770,00	15 596 990,67	15 402 034,64	98,75%
0EK0U Informačné technológie financované zo štátneho rozpočtu – NBÚ	134 485,00	142 723,48	125 327,42	87,81%
0EJ0P Informačná spoločnosť 2014-2020 - MF SR - NBÚ	0,00	3 918 892,40	3 895 710,82	99,41%
E. Systemizácia policajtov v štátnej službe	**232 osôb**	**232 osôb**	**206 osôb***	**88,79%**
	6 875 982,00	**7 042 723,72**	**7 030 330,49**	**99,82%**

BUDGET FOR 2024

According to Act No. 534/2023 on the State Budget for 2024, binding indicators of the state budget for individual chapters were approved and communicated. The National Security Authority's expenditures for 2024 are budgeted within Program 0D9 – Information Security and the interdepartmental subprogram 0EK0U – Information Technology funded from the state budget – NBÚ, totaling €15,881,633.

The office's revenues, as a binding indicator, are budgeted at €20,000, and revenues under source code 72e are budgeted at €2,000.

The budgeted funds will be used by the office to fulfill tasks arising from its role as a central government body responsible for the protection of classified information, cryptographic services, cybersecurity, and trust services. Additional tasks of the office are related to fulfilling commitments from the resolutions of the Government of the Slovak Republic and obligations towards the EU and NATO.

Projects and Achievements

Electronic Services for Processing NBÚ Security Files – eGov Services Improvement:
The primary activities of the project, which is part of the Integrated Infrastructure Operational Program, were in the implementation phase during 2023. The goal is to establish fully electronic services within NBÚ for security clearance processing for citizens and businesses and to build the NBÚ Security Files Processing Information System.

New Projects in 2023

In the fourth quarter of 2023, the office began implementing two additional projects directly funded by the European Union under the Digital Europe program:

- NIS2 Implementation in the Slovak Republic
- Testing and Certification Capacities in Slovakia

Effective Public Administration – CAF Model:

After two years of intensive project implementation, the National Security Authority successfully defended its external feedback and was awarded the significant and internationally recognized title of Effective CAF Model User. In the ranking within the "Central Government Authorities" category, the National Security Authority ranked first.

PUBLIC PROCUREMENT

Analysts from the Transparex.sk portal compiled a ranking of "Responsible Public Procurers." In 2023, the ranking included all state organizations, municipalities, central government bodies, hospitals, state-owned enterprises, kindergartens, and schools. The National Security Authority defended its title as a very responsible procurer with a final grade of A+ and a score of 77.6 points. The assessment indicates that public procurement is conducted professionally, quickly, with a focus on high cost-effectiveness, and ensuring fair competition.

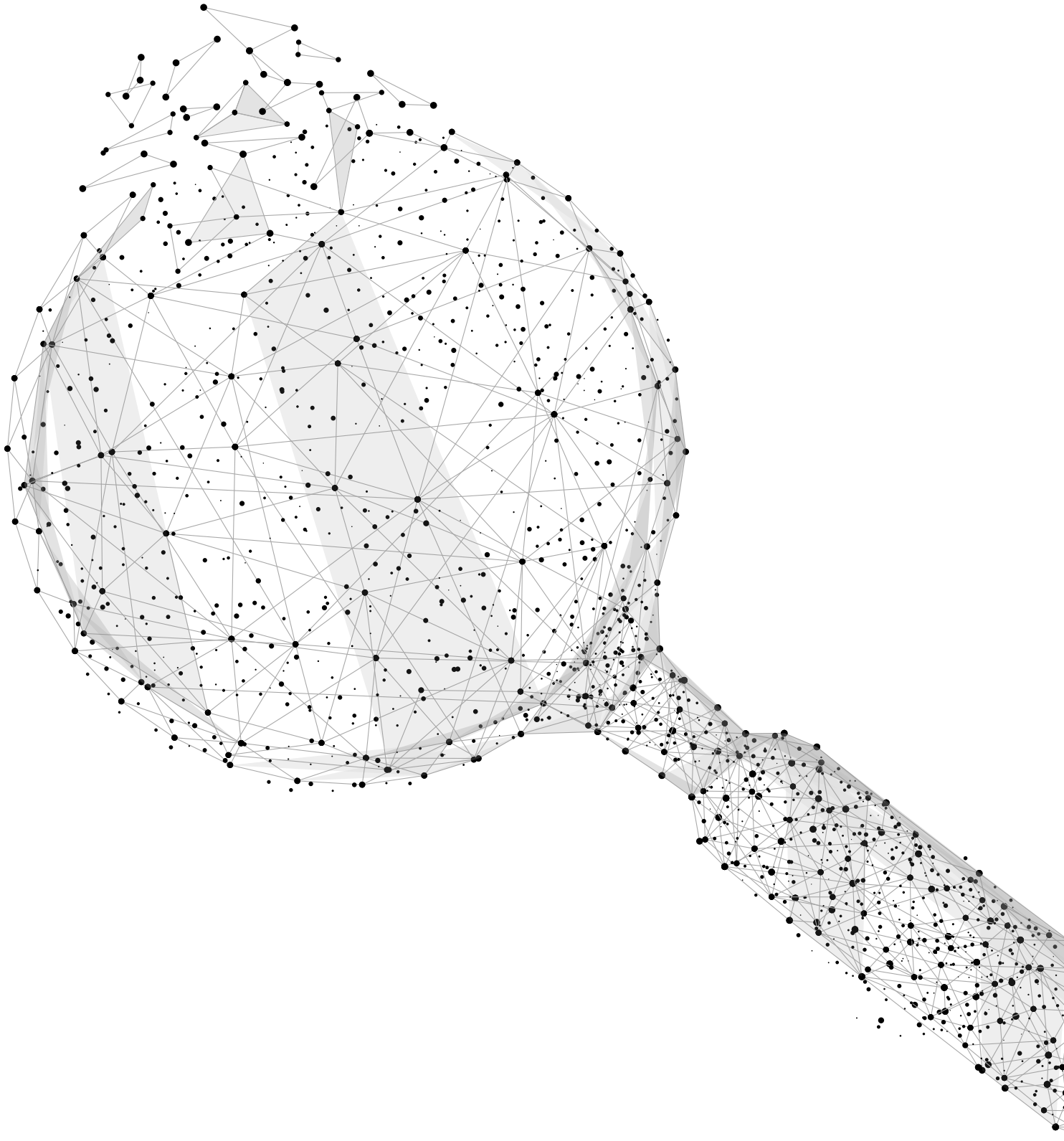
NATIONAL CULTURAL MONUMENT – BRUNOVCE MANSION

The National Security Authority manages the Renaissance mansion from the second half of the 17th century, located in the village of Brunovce in the Nové Mesto nad Váhom district. The mansion is listed in the Central Register of Monuments and in the Register of Immovable National Cultural Monuments. Surrounding the mansion is an English park from the late 18th century.

Due to the unsatisfactory technical condition of this national cultural monument, the office initiated its complete restoration in 2022. The aim is to carry out the reconstruction using funds from the priorities of the Slovak Republic's Recovery and Resilience Plan for the restoration of public historical and protected buildings.

Last year, a restoration research and architectural-historical research of the mansion were conducted. Based on the resulting report, a decision was issued in which the Regional Monuments Office in Trenčín approved the restoration proposal. Currently, project documentation is being prepared, followed by activities related to the construction-technical restoration and the implementation of green measures to extend the lifespan and enable broader use of this national cultural monument.

CONTROL AND AUDIT



CONTROL ACTIVITIES

In 2023, the National Security Authority (Národný bezpečnostný úrad - NBÚ) conducted inspections across 37 entities, including state institutions, businesses, and one international organization. The inspections were categorized according to different laws:

- Protection of Classified Information (Act No. 215/2004): 14 entities (8 state institutions and 6 holders of industrial security certificates)
- Trusted Services (Act No. 272/2016): 4 entities
- Cybersecurity (Act No. 69/2018): 18 entities
- Fulfillment of NATO Membership Obligations: 1 entity

The control teams focused primarily on the comprehensiveness of the measures taken and their coordination across different areas of security.

Findings: 25 of the inspected entities showed deficiencies.

Total Control Findings: 83

- 15 findings in the area of classified information protection
- 67 findings in the area of cybersecurity
- 1 finding in the area of trusted services

SUPERVISORY ACTIVITIES

The NBÚ carried out supervisory activities to ensure that qualified providers of trusted services and the services they offer comply with the requirements set forth in the eIDAS regulation through both ex-ante and ex-post supervision.

These activities mainly involved analyzing compliance assessment reports for regular 24-month audits, overseeing the process of granting qualified statuses, monitoring notifications of changes in service provision by qualified service providers, ensuring that no unauthorized services are being provided, and checking adherence to national legislation regarding trusted services.

- Preliminary Supervision: Reports from four qualified providers of trusted services were analyzed, leading to the issuance of eight qualified statuses for trusted services. One application for two qualified statuses was denied due to non-compliance with eIDAS requirements.
- Follow-up Supervision: Compliance assessment reports from five qualified providers of trusted services were analyzed during subsequent supervision.

Methodological Activities

In May 2023, following the appointment of Slovakia's first-ever caretaker government, the NBÚ provided its members with information on various aspects of classified information protection. This was done through presentations, detailed graphic manuals, and a list of measures to ensure state security and prevent crises.

The NBÚ issues expert opinions and methodological guidelines related to general binding legal regulations. These are provided to state institutions, individuals, and legal entities across all areas of the NBÚ's operations. These opinions and guidelines are anonymized and published on the NBÚ's website.

METHODOLOGICAL ACTIVITIES

In May 2023, following the appointment of Slovakia's first-ever caretaker government, the NBÚ provided its members with information on various aspects of classified information protection. This was done through presentations, detailed graphic manuals, and a list of measures to ensure state security and prevent crises.

The NBÚ issues expert opinions and methodological guidelines related to general binding legal regulations. These are provided to state institutions, individuals, and legal entities across all areas of the NBÚ's operations. These opinions and guidelines are anonymized and published on the NBÚ's website.

In 2023, the NBÚ issued 175 methodological guidelines and expert opinions:

IN THE AREA OF CLASSIFIED INFORMATION PROTECTION	**85**
ON PERSONNEL SECURITY	32
ON ADMINISTRATIVE SECURITY	13
ON INDUSTRIAL SECURITY	17
ON PHYSICAL AND PREMISES SECURITY	10
ON THE SECURITY OF TECHNICAL DEVICES	4
ON SECURITY PERSONNEL	1
ON AERIAL PHOTOGRAPHY	3
ON FOREIGN POWER MATTERS	**9**
IN THE AREA OF CRYPTOGRAPHIC INFORMATION PROTECTION	2
IN THE AREA OF CYBERSECURITY	47
IN THE AREA OF TRUSTED SERVICES	22
CROSS-CUTTING OPINIONS	24

INTERNAL CONTROL

The NBÚ enhanced the professional capabilities of its internal control staff by sending them for training at the Institute for Public Administration. In collaboration with other departments, the Internal Security Section conducted eight internal controls in accordance with Act No. 10/1996 on state administration control.

The controls focused on:

- Compliance with working hours for staff
- Allocation and recording of service weapons and ammunition
- Control of service IDs
- Alcohol testing of staff
- Adherence to obligations under Act No. 278/1993 on the administration of state property
- Administrative security in the protection of classified information

No significant legal violations were identified during these controls, only minor formal administrative issues.

INTERNAL AUDIT

The Internal Audit Department conducted four planned internal audits with the objectives of verifying and assessing:

- Compliance with Act No. 10/1996 on state administration control for 2022 at the NBÚ
- Economy, efficiency, effectiveness, and purposefulness in managing public funds for 2022 and up to August 9, 2023, at the NBÚ
- Economy, efficiency, effectiveness, and purposefulness in managing public funds for 2022 at the Competence and Certification Centre for Cybersecurity

The audits identified nine deficiencies:

- 1 minor, non-systemic deficiency (financial impact unquantifiable)
- 4 medium-severity systemic deficiencies (financial impact unquantifiable)
- 4 medium-severity non-systemic deficiencies (financial impact unquantifiable)

The responsible entities were given deadlines to implement corrective measures and eliminate the causes of these deficiencies, and to submit a list of adopted measures and confirm their implementation in accordance with Act No. 357/2015 on financial control and audit.

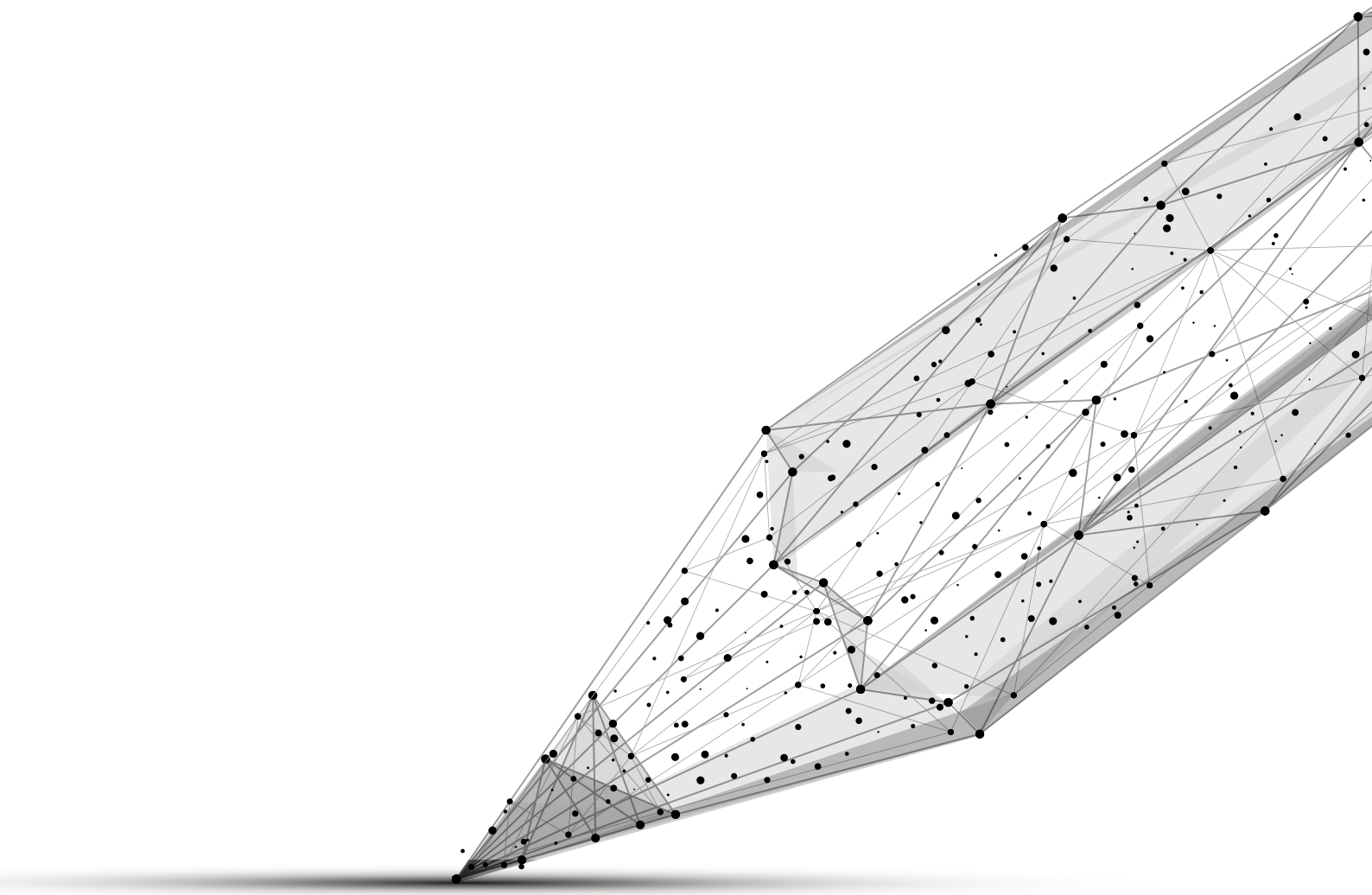
SECURITY RISKS

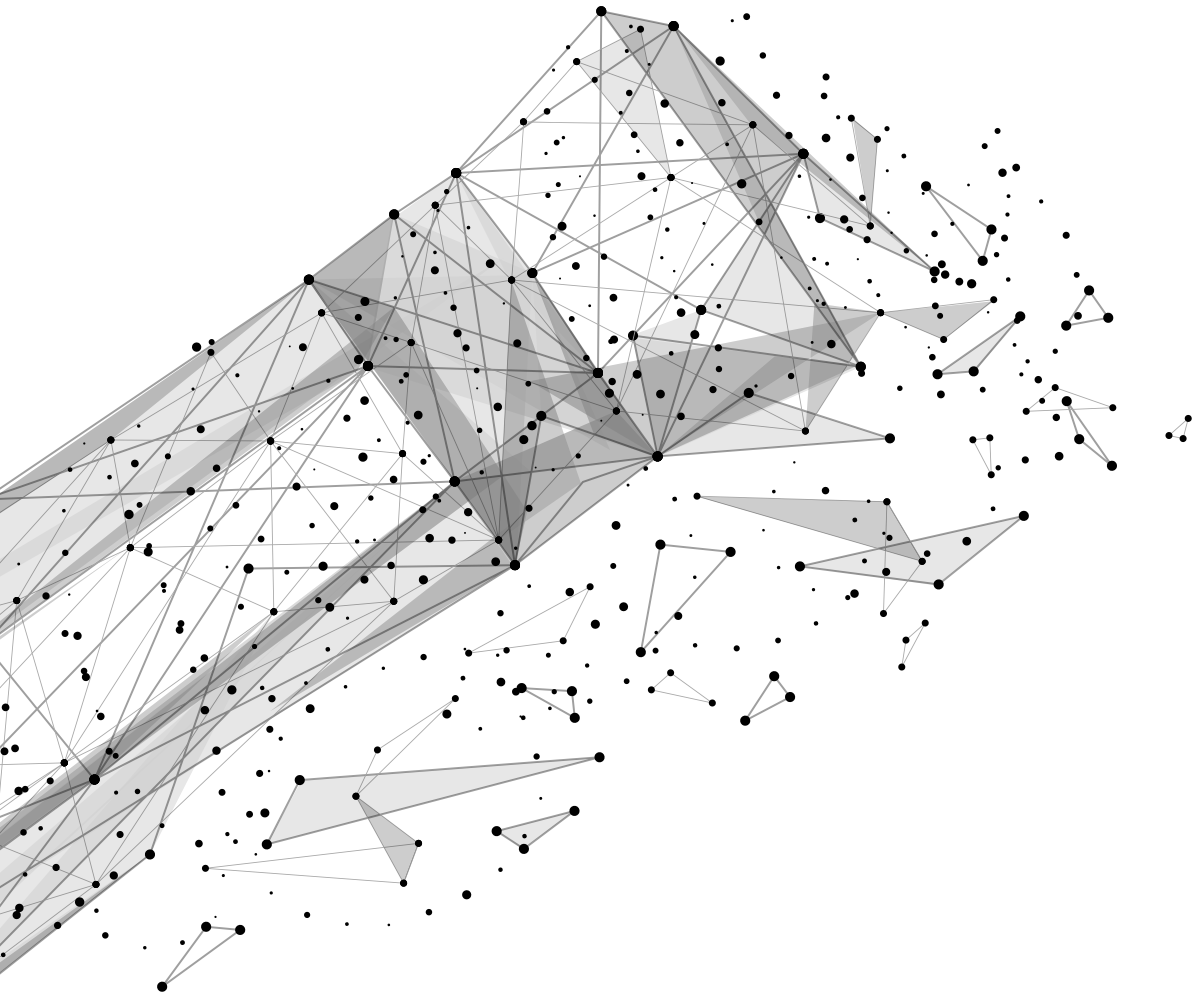
The NBÚ performed its duties in the area of internal security by collecting, analyzing, and verifying information about security risks related to its operations and those of its personnel.

COMPLAINTS AND PETITIONS

The NBÚ received three complaints in 2023, all of which were investigated and found to be unsubstantiated. Another submission labeled as a complaint was determined not to qualify as a complaint under Act No. 9/2010 on Complaints. No petitions were submitted to the NBÚ in 2023.

PRIORITIES FOR 2024





Project Finalization:

- **Electronic Services for the Processing of NBÚ Security Files:** We are finalizing the project focused on improving eGovernment services and are working intensively on three other projects.
- **Enhancing the Efficiency of Public Policy Management in Cybersecurity (2023 – 2024):** We continue to focus on increasing the effectiveness of public policy management in the area of cybersecurity.

Intensive Work on Projects:

- **Building Physical and Premises Security**
- **Implementation of NIS2 in the Slovak Republic**
- **Testing and Certification Capacities in Slovakia**

Additional Priorities:

- **Amendment of the Filing Regulations and Filing Plan:** The office will amend its filing regulations and filing plan during the year.
- **Integration with External Environment:** A key priority is launching the integration of the external environment with the electronic information system for records management. The office will continue to prioritize this integration to ensure seamless operation between the records management system and external entitie