AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

ANNUAL REPORT
2023

St. "Papa Gjon Pali II", No. 3, Floor I
Tiranë, Albania

TABLE OF CONTENTS

MESSAGE OF NATIONAL COORDINATOR AND GENERAL DIRECTOR OF NAECCS

Dear,

It is our pleasure to present to you the 2023 Annual Report of the National Authority on Electronic Certification and Cyber Security (NAECCS). This report provides a detailed overview of our achievements and progress during the year in the field of trusted services and cyber security in Albania.

Our mission is to achieve a high level of cyber security, through the determination of security measures, obligations and rights, as well as a close cooperation between all parties operating in this field. We are committed to guarantee a high level of reliability and security in trusted services, electronic transactions between citizens, businesses and public authorities, increasing the efficiency of public and private services and electronic commerce, to create a secure electronic environment.

In 2023, our activity was focused on several main directions: strengthening the legal framework for cyber security, revising the action plan of the national cyber security strategy, raising technical capacities for the protection of critical and important information infrastructures, expanding cooperation inter-institutional, improving responses to cyber-attacks, as well as developing strategic partnerships with international and governmental organizations.

During this year, Albania experienced numerous cyber-attacks, targeting state institutions and private companies. NAECCS, in cooperation with our partners, has managed to manage these threats with high professionalism, minimizing the damage and recovering the affected services.

Also, we continued the work for the implementation of the Information Security Management System in our institution, based on international information security standards. This implementation plays an important role in the efficient management of information security and provides a strong guarantee for the proper handling of data of critical and important information infrastructures.

We remain committed to our vision to build a secure cyber environment in Albania and to guarantee the reliability of our services for all citizens.

Kind Regards,
Prof. Asoc. Dr. Igli Tafa

INTRODUCTION

The National Authority on Electronic Certification and Cyber Security (NAECCS) was created with DCM No. 141, dated 22.2.2017, has the responsibility of supervising the implementation of Law No. 9880/2008, "On Electronic Signature", Law No. 107/2015, "On Electronic Identification and Trusted Services" as well as Law No. 2/2017, "On Cyber Security" and by-laws issued in their implementation.

OBJECTIVE OF THE REPORT

This document is a report on the activity of the National Authority on Electronic Certification and Cyber Security, for the period January - December 2023.

The purpose of this Annual Report is:

- To present the progress of the activity of the National Authority on Electronic Certification and Cyber Security.
- Analyzing the main priorities of the Authority.
- To identify issues or challenges for the future work of the National Authority on Electronic Certification and Cyber Security.
- To ensure transparency in the activity of the Authority.

The annual report helps convey information to stakeholders, including supporters, donors, authorities, and the public.

The report serves as a tool to evaluate and improve the institution's activity in the future.

I. NATIONAL AUTHORITY ON ELECTRONIC CERTIFICATION AND CYBER SECURITY

NAECCS has the responsibility of supervising the implementation of Law No. 9880/2008, "On Electronic Signature", Law No. 107/2015, "On Electronic Identification and Trusted Services" as well as Law No. 2/2017, "On Cyber Security" and by-laws issued in their implementation.

MISSION

Achieving a high level of cyber security, by defining security measures, rights, obligations, as well as mutual cooperation between entities operating in the field of cyber security.

Guarantees security for trusted services, in particular for guaranteeing reliability and security in electronic transactions between citizens, business and public authorities, increasing the effectiveness of public and private services and electronic commerce, as well as defines the minimum technical standards for data security and networks/information systems, in accordance with international standards in this field, in order to create a secure electronic environment.

OBJECTIVE

The creation of an institution that, through the implementation of the law and international technical standards with zero tolerance, establishing credibility for users of electronic signatures, electronic identification, trusted services, and increases security in networks and information systems in the Republic of Albania.

FUNCTIONS OF NAECCS

1. Registers/accredits the Trusted Service Provider and supervises its activity.
2. Inspects the methods of generating and managing public keys and electronic certificates.
3. Supervises the process of issuing qualified electronic certificates and the implementation of electronic signature, electronic identification and other trusted services.
4. Guarantees standards on the secure identification of individuals to whom qualified electronic certificates are issued.
5. Determines Cyber Security measures at National level.
6. Central point of contact at national level for responsible operators in the field of cyber security and coordinates the work to resolve cyber security incidents.
7. Acts in the capacity of the national CSIRT.
8. Provides methodical assistance and support to responsible operators in the field of cyber security.
9. Conduct awareness and education activities in the field of cyber security.
10. The authority coordinates its activities with security and defense institutions and cooperates with sectorial CSIRTs and international authorities in the field of cyber security, through joint agreements, in accordance with the legislation in force.

II. NAECCS ACTIVITY IN 2023

In 2023, the Authority focused its activity on the following areas:

1. Strengthening the legal framework for cyber security, to protect critical information infrastructures and effective incident management.
2. Expansion of Cooperation and Understanding Agreements with banking and state institutions and with the State of Israel in facing cyber challenges.

3. Preparation of regulations and informative materials regarding Cyber Security
4. Control of critical and important information infrastructures regarding the implementation of Cyber Security measures.
5. Raising capacities for responding to cyber-attacks and building a strong monitoring structure to prevent similar incidents in the future.
6. Building strategic partnerships with international and governmental organizations to strengthen cooperation and avoid cyber crises at the national level.
7. Development of training and awareness programs for cyber security in the public and private sector, to increase awareness and capacities for protection.
8. Efforts to increase the transparency and accountability of NAECCS in its activity, ensuring that its data and reports are accessible and verifiable by the public and other institutions.
9. Use of advanced technology and development of advanced tools to detect, monitor and prevent cyber-attacks effectively.

IMPLEMENTATION OF THE STANDARDS OF THE INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO 27001)

During the year 2023, the National Authority on Electronic Certification and Cyber Security has worked on the implementation of the Information Security Management System in the institution based on the ISO 27001 Standard. The implementation of this standard is a process that ensures a secure approach to information management.

The implementation of ISO 27001 will help the National Authority on Electronic Certification and Cyber Security to ensure a high level of information security and meet international standards in this field.

COOPERATION AND PARTNERS

NAECCS has promoted cooperation with partners whose main focus is Cyber Security by:

- Organizing seminars to share experience and best practices in the field of cyber security.
- Creating joint training and certification programs in cyber security to increase the capacities of employees and their partners.
- Collaborating in joint technological research and development to meet cyber security objectives at the local and international level.

STRENGTHENING OF ADMINISTRATIVE CAPACITIES

Based on a summary of the main needs identified in 2023, NAECCS staff have attended training and certifications in several areas, as follows:

- Cyber Crisis and Communication Workshop – 10 employees
- CompTIA Security + - 12 employees
- Senior Policymaker Cyber Strategy Planning Workshop – 3 employees

- CISSP Training – 10 employees
- Cybersecurity Risk Management and Baseline Security for Organizations – 2 employees
- Risk Assessment Training – 8 employees
- Hacker Fundamentals – 3 employees
- Secure Coding - 3 employees
- Threat Hunting Exercise – 10 employees
- Workshop on governing cyber crisis - 10 employees
- Cyber Defense Strategy Development – 4 employees
- Senior Policymaker Cyber Strategy Planning Workshop – 3 employees
- Cyber Security in Public Administration – 2 employees
- USTI Cybersecurity Policies and Strategy Training Sequence – 3 employees
- ICS Training – 2 employees
- Train the Trainers Course on Cyber Hygiene – 2 employees
- Cyber Diplomacy and Policy Course - 2 employees
- Cyber security governance - 2 employees
- Zero Trust - 2 employees
- Defending against adversary actions – 1 employee
- Seasonal School on Digital Transformation 2023 – 2 employees
- WB3C Training for CISOs of Critical Infrastructure in WB – 1 employee

RESULTS OF REALIZED PROJECTS

During the year 2023, NAECCS has implemented projects in cooperation with national and international organizations as follows:

PROJECT

A decade of raising awareness for children's online safety - workshop to conclude a two-year project.

The National Authority on Electronic Certification and Cyber Security (NAECCS), in cooperation with the International Telecommunication Union (ITU), held a workshop on December 6, 2023, as part of the conclusion of a two-year project launched in September 2021. The main goal of this project was to raise awareness and cooperation on children's online safety, increasing capacity and awareness through training and awareness campaigns for children, youth, teachers, parents and social workers. The workshop brought together representatives from state institutions, civil society, and the private sector to discuss current legislation, reform needs, and highlight the importance of a safer cyberspace for children. The discussions also included the presentation of the results of the activities developed during the project period throughout Albania.

PROJECT RESULTS

The results of the project are as follows:

- Three promotional videos in the Albanian language based on the ITU Guidelines for the protection of children on the Internet, distributed in national online media, aimed at educating children, youth, parents, teachers and industry operators.
- Manual for children, distributed in 12 districts of Albania for the awareness of children and young people about online risks.
- Preparation of the "Train the Trainer" manual for parents, teachers and guardians to strengthen the protection of children on the Internet.
- Sharing a Unified Message with key industry players to increase online safety for children.
- Drafting an Impact Report to assess awareness and learning before and after the trainings.
- Organization of 12 online workshops for children and young people in order to raise awareness and engage youth communities in the consultation process on initiatives related to the protection of children online, as well as 15 workshops for parents and teachers to increase their digital skills, in order to be able to protect children and young people online.
- Creation and distribution of a brochure with tips on internet safety.
- Organization of 5 workshops with industry stakeholders to increase cooperation in protecting children online.
- Development of 5 workshops for ICT professionals and 12 capacity building activities for teachers and government experts on relevant skills required to strengthen online safety for children in the context of ITU focus areas.
- Preparation of two reports: Report on Priority Assessment and Report on the Implementation Plan for Child Protection Policies on the Internet in Albania.

MAIN ACTIVITIES DURING 2023

3- day seminar "Senior Policymaker Cyber Strategy Planning"

The 3-day seminar "Senior Policymaker Cyber Strategy Planning" was organized by the National Authority on Electronic Certification and Cyber Security in cooperation with the US Department of State and MITRE Corporation on January 24-26, 2023.

The purpose of the 3-day workshop was to finalize the development of the framework for a National Strategy for Cyber Security, which includes the formulation of policy goals, the identification of supporting initiatives for each goal, the identification of actors for each initiative, and recommendations for challenges and overcoming them for the implementation of activities.

The seminar, led by MITRE Corporation, focused on the role of each security and defense institution in designing security strategies and policies for managing cybersecurity issues, as well as aligning strategic plans with best practices of the US- widow.

CISSP training

Within the framework of the new strategic plan for strengthening cyber security at the national level, with the support of e-GA, a series of trainings was initiated during 2023, dedicated to increasing the professional capacities of the staff responsible for cyber security at the National Authority on Certification Electronic and Cyber Security, as well as in some of the country's critical information infrastructures.

In this context, on February 27 - March 3, 2023, representatives of NAECCS and representatives of some of the critical information infrastructures successfully completed the CISSP training.

Conference "Challenges of Cyber Security in Albania"

In the framework of the International Safe Internet Day, the National Authority on Electronic Certification and Cyber Security (NAECCS) in cooperation with the OSCE Presence in Albania, USAID / DAI, the National Agency of Information Society (NAIS), the Albanian Association of Banks, Soft&Solution, R&T Group, One Telecommunications and DigitALB organized the conference "Challenges of Cyber Security in Albania", near MAK Albania hotel on 07.02.2023.

The purpose of the conference was to increase the level of cyber security in the country in implementation of the new Strategic Plan for cyber security, by addressing current cyber security challenges, as well as strengthening cooperation with strategic partners and collaborators, considering also the valuable contribution of field experts from the diaspora.

Participants included government representatives, diplomats, and industry leaders who discussed raising awareness and working together to minimize damage from cyber-attacks. The conference also included sessions on critical infrastructure protection and the overarching importance of enhancing cyber resilience.

Training: Increasing Human Capacities in the field of Cyber Security

On 11.04.2023, within the framework of the new strategic plan for strengthening cyber security at national level, the National Authority on Electronic Certification and Cyber Security, developed a training dedicated to increasing the professional capacities of staff responsible for cyber security of critical infrastructures and important information in place.

The organized training included two parallel sessions dedicated to strengthening the cyber security of information infrastructures. In the first session, the staff of new critical and important infrastructures, identified in 2022, got acquainted with the current legal framework, the importance of setting up sectoral CSIRTs, the responsibilities and processes of identifying infrastructures, as well as cyber security measures that must be implemented. The second session included practical exercises "Tabletop Exercises" for representatives of existing infrastructures, where different scenarios were discussed to strengthen awareness, technical capacities and the design of security procedures to manage and prevent cyber incidents.

Signing of the Cooperation Agreement in the field of Cyber Security between NAECCS and the United Arab Emirates

On 05.04.2023, the Cooperation Agreement in the field of cyber security was signed between NAECCS and the United Arab Emirates. With the signing of this important Agreement, NAECCS started a new chapter of cooperation with the strategic partners of the United Arab Emirates, towards securing the invisible borders of Albania's cyberspace, through the exchange of information, the exchange of best practices and the strengthening of human capacities.

Regional cyber security exercise

4- day cyber training, organized by the Estonian e-Governance Academy, CybExer Technologies, National Agency of Information Society (NAIS), National Authority on Electronic Certification and Cyber Security (NAECCS) and other competent security authorities, with the support of the European Union, was held in Tirana where cyber security experts from Albania, Montenegro, and North Macedonia participated. The Albanian team, led by representatives of NAIS and NAECCS, with participants from other security institutions and critical information infrastructures, showed excellent skills in responding to a cyber-attack simulation, ranking first.

The activity was attended by the President of the Republic of Albania H.E.Mr. Bajram Begaj together with the President of the Republic of Estonia, H.E.Mr Alar Karis and the Ambassador of the European Union H.S. Mrs. Christiane Hohmann.

TTX and Cyber Drill for the Transport and Energy sector

On November 6-7, 2023, in cooperation with Risi Albania, the training on "Cyber Security Policies and Crisis Management" was held for the transport and energy sectors. During this two-day training, presentations were made regarding the legal framework, strategy, policies, the necessary security measures that must be taken by information infrastructures and the needs for cyber governance. An important part of this training was also the development of two Tabletop Exercises for the management of cyber incidents and crises, industrial cyber threats that include attacks on IT, OT and IoT systems, as well as the simulation of the "Phishing" attack, where in the developed scenarios cases of malware infection (malicious programs) were analyzed. Cyber Drill was also organized through the FISA.al platform, where concrete exercises on the identification and management of cyber incidents were conducted.

TTX and Cyber Drill for the Financial and Insurance sector

NAECCS, focused on increasing the level of cyber security in information infrastructures at national level, during 2023 has supported the Operators of Critical and Important Information Infrastructures to increase their professional and technical capacities.

With the support of our partner Risi Albania/Helvetas and the contribution of NAECCS experts, on November 23-24, 2023, the training activity with the financial/banking sector took place.

The two-day activity focused on the development of various TTX scenarios, dedicated to this sector, and the participants were involved in the Cyber Drill exercise, showing their skills in solving cyber incidents based on the relevant procedures.

TTX and Cyber Drill for independent institutions, the Water Sector, NAIS and the State Police

In continuation of NAECCS's objective of increasing capacities as one of the main pillars for the protection of information infrastructures with the support of our partner Risi Albania/Helvetas and the contribution of the Authority's experts, held on December 20, 21 and 22, 2023, the training of provided on the topic of "Cyber Security Policies and Crisis Management" for Independent Institutions, the US Sector, NAIS and the State Police.

For the very importance that these sectors have in terms of the information infrastructures they manage, during this three-day training, presentations were made regarding the legal framework, strategy, policies, the necessary security measures that must be taken by the information infrastructures and the needs for cyber governance.

An important part of this training was the development of three different TTX scenarios for cyber incident management. Also, 2 days of cyber training (Cyber Drill) were held with concrete exercises on cyber incident management, via the FISA.al platform.

2023 COOPERATION AGREEMENT AND MEMORANDUM

- Cooperation Agreement with Raiffeisen Bank.
- Cooperation Agreement with the Electricity Distribution Operator (OSHEE).
- Cooperation Agreement with Union Bank.
- Cooperation Agreement with Tirana Bank.
- Cooperation Agreement with the First Investment Bank.
- Cooperation Agreement with the Assembly of the Republic of Albania.
- Cooperation Agreement with the Transmission System Operator (OST).
- Cooperation Agreement with the Albanian Post.
- Cooperation Agreement with the Armed Forces Academy.
- Cooperation Agreement with the Albanian Association of Banks (AAB).
- Cooperation agreement with Israel.
- Memorandum of Understanding with the Cyber Security Council of the United Arab Emirates.
- Memorandum of Understanding with 4IG.

III. DIRECTORATE OF CERTIFICATION, POLICY AND LEGAL AFFAIRS

The Directorate of Certification, Policy and Legal Affairs has as its object of activity the creation of a secure cyber environment in networks and information systems, as well as guaranteeing the security of electronic transactions, using trusted services through the drafting of policies and draft the necessary legal acts in line with the objectives of the Authority.

The Directorate of Certification, Policies and Legal Affairs consists of the director of the department and two relevant structures:

- Certifications and conformity sector.
- Policy and legal affairs sector.

CERTIFICATIONS AND CONFORMITY SECTOR

1. Training and participation activities in:
   - In the *"CompTIA Security+"* training held on February 20 - 24, 2023;
   - In the activity of *"Assistance to the Albanian National Security Agency"* organized by the National Authority for the Security of Classified Information in cooperation with TAIEX on April 24 - 28, 2023;
   - In the *"Cyber Crisis Governance"* activity organized by NAECCS in cooperation with CRDF Global and the C3I Cyber Security organization, Corporate Security and Crisis Management Initiative on July 11 - 12, 2023.
2. The identification of processes, steps and by-laws has been carried out to fulfill the mission of the Certification and Conformity Sector;
3. Research was done on models, related to the preparation of documents for by-laws, within the draft law "On Cyber Security" and the draft law on "Electronic Identification and Trusted Services."
4. Within the draft law "On Cyber Security" the draft document was drawn up:
   - *Audit Questionnaire for Critical and Important Information Infrastructures" (transposition of ISO 27001-2022).*
   - *Instruction on determining the application procedure and criteria for the registration of conformity assessment bodies at the National Cyber Security Authority.*
5. Within the draft law "On Electronic Identification and Trusted Services" the draft document has been prepared:
   - *Instruction on determining the application procedure and criteria for the registration of conformity assessment bodies National Cyber Security Authority.*
6. The process of reviewing the documentation for the subject, which submitted the request to benefit from the status as a qualified trusted service provider, has been started.
7. Drafting of documents, memos according to the institution's needs and the directors’ requirements.

POLICY AND LEGAL AFFAIRS SECTOR

Throughout the year 2023, the Policy and Legal Affairs Sector has carried out the following tasks:

1. Within the process of the country's integration into the European Union, work has continued to update the current legal basis, which includes Law No. 9880/2008, "On electronic signature", Law No. 107/2015, "On electronic identification and trusted services", in full compliance with the European Regulation eIDAS No. 910/2014, "On electronic identification and trusted services for electronic transactions in the internal market", as well as Law No. 2/2017, "On cyber security" in high-level harmonization with

Directive No. 2022/2555 of Parliament and Council dated December 14, 2022, "On measures for a common high level of cyber security throughout the European Union, which has amended Regulation (EU) No. 910/2014 and Directive (EU) No. 2018/ 1972, as well as repealed Directive (EU) No. 2016/1148. (NIS 2).

The draft law "On cyber security" was sent to the Prime Minister in December 2023 for the continuation of further procedures for the approval of the latter, after the public consultation process was carried out in the electronic register of public consultation and meetings with interest groups.

The draft law "On electronic identification and trusted services", the public consultation process has been completed (7.12.2022-10.01.2023). After the end of the public consultation, it continued with the reflection of the comments received from the institutions and the final draft of the draft law was sent electronically to the Prime Minister on 04/07/2023 for further procedures. The draft law will be reviewed in its entirety, taking into consideration the technical nature of the constituent elements and in the framework of the reengineering of services.

2. Legal acts approved during 2023:
   - The internal regulation "On the organization and functioning of NAECCS", approved by Order No. 201 dated 20.11.2023.
   - Instruction No. 2, dated 13.11.2023, "On some changes in instruction No. 1, dated 15.03.2023, "On the termination of the activity of the Qualified Trusted Service Provider and the Transfer of the Service."
3. In the framework of integration into the European Union, a contribution has been made in the following areas:
   - Reporting on chapters 10, 20, 24, 31 within the framework of GNPIE;
   - Participation in meetings within GNPIE;
   - Completion and reporting on PPAP and PKIE 2023-2025, 2024-2026;
   - Reporting in the framework of drafting the Roadmap of the Code of Law for chapters 23, 24.
   - Completion and reporting related to EISP (European Integration Semester Package)
   - Preparation of material for the meetings of the innovation sub-committee, information society, social policies (meetings 14 and 15).
   - Participation in bilateral meetings, in Brussels, for Chapter 10;

4. Drafting, revision, improvement of agreements at national level and at international level in the field of cyber security.

   During 2023, 10 cooperation agreements (national) and 3 MoUs (Memorandum of Understanding) were signed.

5. Following court proceedings where the Authority is a party to the trials.

During the year 2023, 4 trials were conducted, 3 of which have been completed and won by NAECCS, 1 is in process, the court declared incompetence and transferred it to the competent court.

6. Drafting of legal reports, various written correspondences with the institutions as needed, as well as reports whenever required in accordance with the activity of the institution.

7. In the framework of the obligations defined in the legislation for the declaration of assets and the prevention of conflict of interest, it is reported periodically and annually to the HIDAACI.

8. Participation in:

   - ✓ Regional conference Cyber Balkans Project on EU International Cybersecurity Law November 20-22, Podgorica ("Regional conference Cyber Balkans project on EU International Cybersecurity law").
   - ✓ "Workshop on Cyber Crisis", July 11-12, Tirana (Governing Cyber Crisis Workshop).
   - ✓ Seminar "On National Cybersecurity Legislation" June 6-7, Tirana (Seminar on National Cybersecurity Legislation)
   - ✓ 3rd EC Trust Services Forum (EC-3rd Countries Trust Services Forum).
   - ✓ iPROCEEDS-2 workshop were held on September 26-27, 2023 in Tirana.

IV. DIRECTORATE OF CYBER SECURITY GOVERNANCE, CONTROL AND STRATEGIC DEVELOPMENT

The Directorate of Cyber Security Governance, Control and Strategic Development aims to ensure the good governance of cyber security through the drafting of strategic plans and their monitoring, the identification of information infrastructures and their categorization, the drafting of cyber security measures for information infrastructures, their control and monitoring, awareness and capacity building, as well as monitoring the activity of qualified trusted service providers to guarantee electronic transactions in the internal market, through the use of trusted services.

Directorate of Cyber Security Governance, Control and Strategic Development:

1. Sector of cyber security governance and control
2. Sector of strategic development, communication and identification of infrastructures
3. Sector of statistics, models and analysis of indicators

SECTOR OF CYBER SECURITY GOVERNANCE AND CONTROL

In fulfillment of functional duties as well as in implementation of Law No. 2/2017, "On Cyber Security", Decision of the Council of Ministers No. 553, dated 15.07.2020, "On the approval of the list of critical information infrastructures and the list of important information infrastructures", amended, and the regulation **"On the content and method of documenting security measures** (*V. 2.0, approved with Order No. 10/2022*), the cyber security governance and control sector during the period **January-December 2023**, has carried out continuous cyber security controls near critical and important information infrastructures.

Through 2023, the number of on-site checks on critical and important information infrastructures quadrupled.

Below is a summary of the cyber security checks carried out by the Cyber Security Governance and Control Sector for the year 2023.

Operators	**Controlled**	**Self-declaration**
Operators of Critical Information Infrastructures	26	32
Operators of Important Information Infrastructures	23	22
Total Infrastructure Operators	49	54

Table 12. Cyber security controls

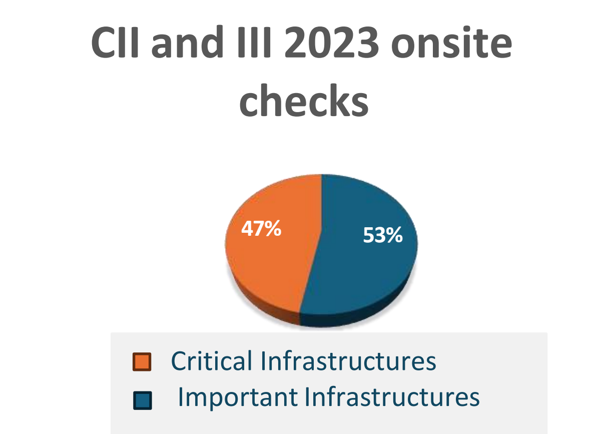


Figure 24. On-site controls for operators of critical and important information infrastructures.

REGULATION ON THE CONTENT AND WAY OF DOCUMENTING SECURITY MEASURES V.2.0 AND ADDITIONAL MAIN TECHNICAL MEASURES (BASELINE)

The cyber security governance and control sector performs controls based on the regulation **"On the content and manner of documenting security measures** (*V. 2.0, approved by Order No. 10/2022)*" and the main additional technical measures (Baseline) of which must be implemented by all critical and important information infrastructures in the country and these additional technical measures include:

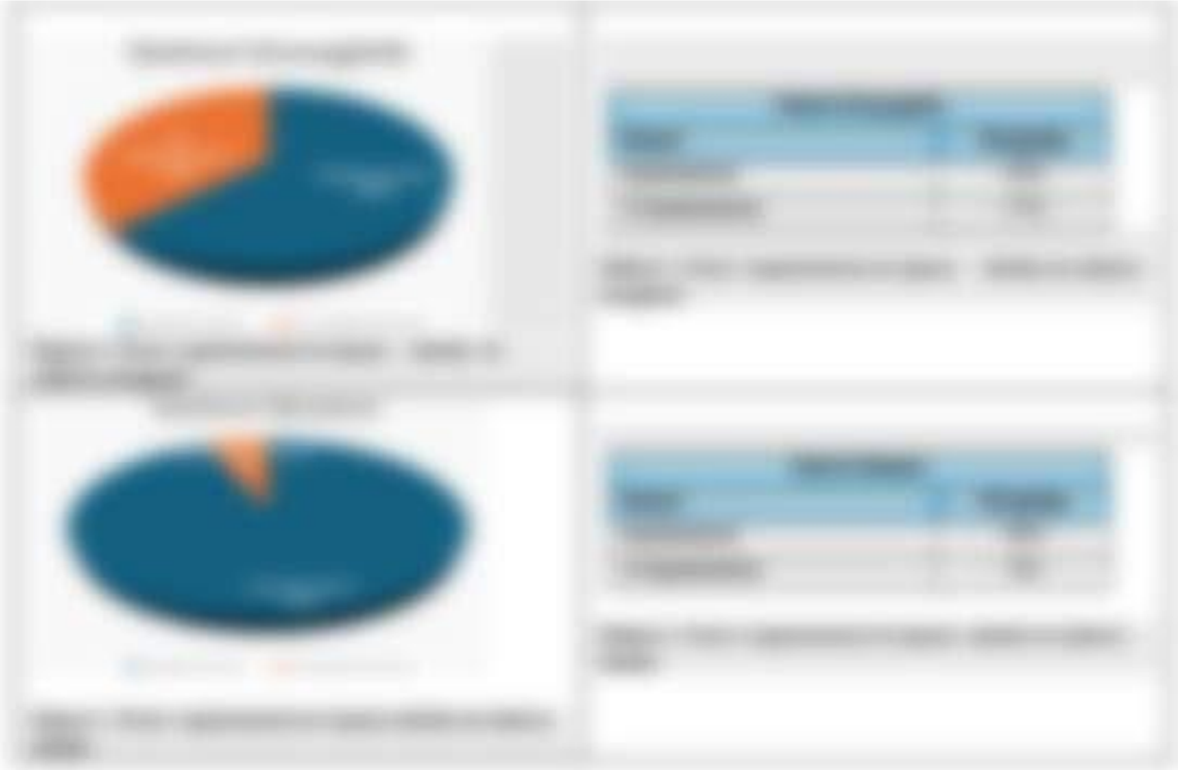
- To install network perimeter devices that perform deep traffic analysis based not only on access list rules but also on its behavior (Firewalls).

- To consider "High-Availability" schemes in "core-network" devices at the perimeter level (firewall), at the routing level (L3) and packet switching (L2) and at the level of physical lines (L1).
- To take measures for the use of data mirroring techniques (RAID 1/5/6/10) to avoid the loss of sensitive data.
- To take measures to avoid "Single Point of Failure" in your critical and important services.
- To apply traffic filters in the case of remote access to hosts (employees/third parties/customers).
- To implement solutions that filter, monitor and block malicious traffic between Web applications and the Internet, Web Application Firewall (WAF).
- To conduct traffic analysis at the "behavior" level for end devices.
- To design the "Identity Access Management" user access management solution to control the identity and privileges of users in real time according to the "zero-trust" principle.
- To implement an automated system for managing and filtering logs in order to identify alerts in real time.
- If you have a development department, perform software development testing (stage-ing) in an isolated environment separated from the production environment.
- To take measures to implement a system that controls the security parameters of an end system, not allowing the latter to be part of your network if these parameters are below the "Baseline" level previously given by you? (System which checks the lack of patches, Anti-Virus updates, etc.).
- To Logically isolate (in different VLANs) Database and Web services (if they are hosted in your environment).
- To take measures to raise DNS_SEC to avoid DNS Amplification attack and DNS_Poisoning attack.
- To implement and test the Disaster Recovery Site for the most important and critical services.
- To take measures to replace or isolate "End of Life" systems installed in your equipment.
- To take measures for the identification and effective management of assets and to carry out the assessment of risks by recording:
    - Antiquity
    - Affecting of C/I/A (Confidentiality/ Integrity/ Availability
    - Identified Vulnerabilities (CVEs)
- To draw up detailed plans and procedures for the management of cyber incidents.
- To take measures to isolate the wireless network from the rest of the network.
- To implement employee awareness campaigns regarding cyber security and the most frequent attacks such as Phishing etc.
- Conducting tests for assessing the security of applications and networks (penetration test) and draw up a plan for dealing with identified problems.
- Conducting internal or third-party checks/audits for information security in your infrastructures.
- To check if the Email system does not have anti-spoofing features configured: DMARC/SPF/DKIM.
- To check if there is a Web Service that operates on the http protocol.

- To check if there is a Whitelist of allowed IP addresses set up in the firewall.
- To use random password policy for local users/administrators (e.g. as Microsoft's LAPS).
- Use the Data Leakage Prevention platform to prevent information leakage.
- To use the protection technique against DoS/DDoS attack.
- To use the technique of Port Security on Switches where the maximum number of MAC Addresses is 1 for simple users and a limited number for IT or Cyber Security experts.

Based on the regulation **"On the content and method of documenting security measures (V. 2.0, approved by Order No. 10/2022)"** and Baseline of additional technical cyber security measures, controls exercised, as well as follow-up of critical and important infrastructures, the cybersecurity governance and control sector has evaluated their implementation at the infrastructure level, as well as at the sectoral level.

The level of implementation of technical security measures by critical and important information infrastructures at the sector level is presented below.



[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

In cooperation with the critical and important information infrastructures, the analysis was carried out on the budgets dedicated to cyber security for the year 2023 and 2024, as well as the investments in cyber security for the year 2023.

From the data collected by the operators of critical and important information infrastructures, it results that the budget, as well as the planning for projects in the field of cyber security has a significant increase over the years, pointing out the awareness of the infrastructures for concrete investments in the field of cyber security.

Below is a summary of the dedicated budget and investments for cyber security at the sector level.

[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]

[illegible]

[illegible]

SELF STATEMENTS OF CRITICAL AND IMPORTANT INFORMATION INFRASTRUCTURES

According to self-reported critical and important information infrastructures, there is a small increase in terms of dedicated cybersecurity job positions for each sector.

CYBER SECURITY VULNERABILITY ASSESSMENT (GAP ANALYSIS)

The cyber security governance and control sector has carried out the security assessment of technical measures, based on emergency security measures and the New Program for the assessment of cyber security vulnerabilities (GAP Analysis).

During the year 2023, the cyber security risk assessment was carried out in 11 important institutions in the field of security and defense.

The Cyber Security Governance and Control Sector has implemented the **CISA CSET TOOL** for assessing the level of implementation of CII& III security measures.

Functionalities of CSET TOOL

- Effective control of the implementation of security measures by CII and III
- Analyzing cyber security vulnerabilities of CII and III
- Assessment of the level of cyber security (Cyber Resilience), as well as risk assessment of CII and III
- Creation of dedicated profiles for all critical and important information infrastructures, according to specific sectors
- Generating reports (statistically/graphically) on the cyber security level of infrastructures
- Recommendations for improving weaknesses identified during inspection

ADMINISTRATIVE SANCTIONS

The sector of governance of cyber security and control, during the year 2023, drafted *"Instructions for the methodology of determining administrative penalties in the process of control of critical and important information infrastructures"*, approved by the General Director with No. 179 Prot., date 03.03.2023.

After carrying out the control process *"On the evasion of the implementation of recommendations and corrective measures as well as the verification of the implementation of some technical measures"*, the following were sanctioned with a fine:

Infrastructure	**Number**	**Income for the state budget from fines**
Critical Information Infrastructure	4	**3 600 000 ALL**
Important Information Infrastructures	2	

VERIFICATION OF QUALIFIED TRUST SERVICE PROVIDERS

Qualified Trusted Service Providers (QTSP) have the legal obligation to periodically report on their activity to NAECCS.

QTSP NAIS

During the period **January-December 2023**, **QTSP NAIS** has issued: **5293** Electronic certificates with electronic signature for Public Administration
18504 Electronic certificates with electronic signature for Private Entities
3834 Electronic certificates for the e-prescription system
102792 Electronic certificates for the fiscalisation project for private production entities
800 Electronic certificates for the fiscalisation project for state production institutions
2700 Electronic stamp for public administration

TRAININGS

The Cyber Security and Control Governance Sector has conducted during 2023, dedicated trainings with operators of critical information infrastructures and important information infrastructures, identified for the first time in VKM No. 761, dated 12.12.2022.

The focus of the trainings was on the following issues:

- Familiarity with the legal framework of cyber security in the Republic of Albania
- New Strategic Plan for Cyber Security
- CSIRT life cycle management
- Benefits of setting up CSIRT
- Categorization of cyber incidents
- Organizational and technical security measures to be implemented by CII and III
- Cyber Security Controls

SECTOR OF STRATEGIC DEVELOPMENT, COMMUNICATION AND IDENTIFICATION OF INFRASTRUCTURES

The sector of strategic development, communication and identification of infrastructures has important responsibilities for cyber security, identifying and classifying new critical and important information infrastructures and drafting the National Strategy for Cyber Security. It also coordinates the work with other institutions for the monitoring and implementation of the Action Plan of the National Cyber Security Strategy. By taking actions to increase the capacities and cyber security in the country. Plans and organizes specific trainings as well as meetings with national and international actors in the field of cyber security. Among the main objectives, the following were achieved:

STRATEGIC DEVELOPMENT

- **Contribution to the National Security Strategy:** The sector is engaged in the drafting process of the National Security Strategy, led by the Ministry for Europe and Foreign Affairs, contributing to the issues of cyber security, cybercrime and cyber diplomacy according to the relevant pillars of the draft strategy. NAECCS's contribution is included in the National Security Strategy document.
- **Monitoring Report of the National Strategy for Cyber Security:** The sector has drawn up the Monitoring Report of the National Strategy for Cyber Security for the year 2022, after the analysis made regarding the implementation of the 2020-2025 Action Plan. In the framework of this process, the realization of the activities planned for each of the institutions responsible for the implementation of the Action Plan of the National Strategy for Cyber Security 2020-2025 was monitored, for the four goals of the policy, giving a description of the activities carried out as well as draw relevant conclusions and recommendations. This process was carried out in cooperation with the actors of the Action Plan of the National Strategy for Cyber Security 2020-2025, who, in response to the letters sent by NAECCS, provided information on the implementation of the activities undertaken by them in accordance with goals and objectives of the strategy.

- **Preparation of the Action Plan for SKSK 2024-2025, as well as work coordination and meetings with relevant institutions related to this process.**
  The sector has worked intensively for the drafting of the 2024-2025 Action Plan, identifying the priorities and needs in terms of cyber security at national level, based also on the current level of implementation of the activities of the Action Plan of the National Strategy for Cyber Security 2020-2025, in order to plan new activities and commitments that must be carried out in accordance with the goals and objectives of the National Cyber Security Strategy. In this context, the sector team has also coordinated with the institutions responsible for the implementation of the Action Plan of the National Strategy for Cyber Security 2020-2025 and the new institutions involved, to collaboratively determine the activities for each of them according to specific objectives and needs. Currently, the new Action Plan for SKSK 2024-2025 is in the process of approval.

EUROPEAN INTEGRATION

The sector has carried out reports within the European integration process for the planned meeting of **Subcommittee 14, *"Innovation, Information Society, and Social Policies", as well as chapter 10 "Information Society and Media" and chapter 20 "Enterprises and Industrial Policies" "***, where during the analytical review process of the relevant acquis, periodic reports were made, as well as it was reported in the bilateral meeting for the Subcommittee in February 2023 online, while for chapter 10 and 20, the bilateral meetings took place in the offices of the European Commission in Brussels, where reported on the institutional framework, current policies, legal framework and future plans in terms of strengthening cyber security at the national level.

METHODOLOGY FOR THE IDENTIFICATION AND CLASSIFICATION OF INFORMATION INFRASTRUCTURES

The sector has drafted the new Methodology for the Identification and Classification of Critical and Important Information Infrastructures in accordance with the guidelines of the European Union and Directive (EU) 2022/2555. This methodology aims to define the steps and criteria for the identification and classification of information infrastructures starting from the critical service. In function of the work for the drafting of supplementary documents of the methodology, such as the block-schemes of the classification of infrastructures, the new questionnaire was drawn up in accordance with the criteria and indicators defined in the draft methodology. As part of the work to determine the thresholds for each critical sector according to the criteria and indicators established for the classification of infrastructures, letters have been sent to some of the operators of critical and important existing information infrastructures to obtain the necessary information in accordance with the new methodology of Identification and Classification of Information Infrastructures draft. Following several consultation processes carried out in 2024, the analysis of the data collected for the drafting of the final draft of the methodology, including the criteria and thresholds defined for critical services, will be done.

SECTOR OF STATISTICS, MODELS AND ANALYSIS OF INDICATORS.

The Department of Statistics, Models and Analysis of Indicators performs the following tasks:

a. Analyzes cyber security indicators in order to identify trends, patterns and potential cyber threats;
b. Processes and administers statistical data according to the functions of the Authority;
c. Develops and implements effective models for the distribution of information on the best practices of cyber security, in accordance with international practices in the field;
d. Administers and manages the data conveyed by the monitoring and analysis systems, in relation to the systems administered by the operators of critical and important information infrastructures;
e. Creates threat models based on statistics of critical infrastructures and predicts the security risk on these infrastructures;
f. Drafts and publishes all the latest events and developments in the field of security, as well as prepares and publishes weekly and monthly newsletters.

Throughout the year 2023, the sector of statistics, analysis models and indicators has carried out the following tasks:

In implementation of the legislation in force in the field of cyber security, the National Authority on Electronic Certification and Cyber Security (NAECCS) has prepared a total of:

- 12 monthly reports,
- 4 3-month reports, and
- 1 annual report, throughout the year 2023 as a need to reflect the vulnerabilities of important and critical information infrastructures in the cyber ecosystem at the national level, defining cyber security countermeasures case by case.

Authorized sources and platforms were used to monitor vulnerability and assess the level of security of CII and III, but also of other institutions. The monitored infrastructures belong to the transport, banking, digital, financial, energy and public sector infrastructures.

These reports reflect, from a statistical point of view, the monitoring data carried out, analyzing and categorizing the results of the findings according to sectors, vulnerabilities, and risk vectors, throughout the year 2023. The reports also identify problems according to sectors in general, addressing the needs for increased capacities, for investment and technology.

The reports are based only on the scanning and analysis of the samples, which have been made available to the Authority. These reports do not guarantee all possible vulnerable cases of CII/III, due to the limited space for analysis, which was available to NAECCS.

CYBER SECURITY ASSESSMENT AT THE SECTORIAL LEVEL

The Sector of Statistics, Models and Analysis of Indicators has carried out an assessment of the security level of critical sectors, which is based on the following 3 components:

- The risk component of compromised systems,
- The due diligence component,
- User behavior component.

These three pillars are analyzed for each infrastructure and then averaged to determine the level of security, where a high rating indicates a high level of security and a lower cyber risk, while a low rating indicates a high risk. Averaging at the sector level helps in the overall safety assessment.

The analysis of the data related to the assessment of the level of security represents a consistent improvement in all critical sectors. The increase in the level of security results from the implementation of the corrective security measures evidenced in the control reports, the increase of human capacities through specialized training and the increase of awareness on security issues, as well as the improvement of technological capacities and security systems.

These measures have contributed to an increase in the overall level of safety in all critical sectors, proving the importance of a comprehensive and continuous approach to risk management and safety improvement.

EVENTS

Promotional materials

Throughout the year 2023, in implementation of the public communication plan, the realization and publication on the social networks of the National Authority on Electronic Certification and Cyber Security of promotional materials for the awareness of the community for increasing the level of cyber security was carried out.

Also, bulletins, news and articles have been periodically drafted and published, based on the analysis of the current situation of ICT and cyber security, on the official social media communication channels of the Authority.

WEEKLY/MONTHLY BULLETIN

Throughout 2023, the following have been prepared:

- 12 Monthly Bulletin
- 50 Weekly Bulletin

January 2023	**February 2023**	**March 2023**
 Cyber Security News Bulletin January 2023	 Cyber Security News Bulletin February 2023 CYBER SECURITY A NATIONAL PRIORITY! A MEMORANDUM OF UNDERSTANDING IS SINGED BETWEEN AKCESK - ISRAEL NATIONAL CYBER DIRECTORATE	 CYBER SECURITY NEWS BULLETIN March 2023 RAISING CAPACITIES OF CRITICAL INFRASTRUCTURES - IN THE FOCUS OF NAECSS'S ACTIVITIES TAIEX WORKSHOP ON CYBER SECURITY INCIDENTS
April 2023	**April 2023**	**May 2023**
 CYBER SECURITY NEWS BULLETIN April 2023 NATIONAL CYBER SECURITY ACADEMY RSA CONFERENCE PATCHING ALERT	 CYBER SECURITY NEWS BULLETIN April 2023 LOCKED SHIELDS PATCHING ALERT	 CYBER SECURITY NEWS BULLETIN May 2023 PATCHING ALERT

May 2023 	June 2023 	June 2023
July 2023 	July 2023 	August 2023
August 2023 	September 2023 	September 2023

October 2023	October 2023	November 2023
 CYBER SECURITY NEWS BULLETIN October 2023 Content: Security Policies and Crisis Management for the Health Sector. AKCESK participates in Cyber Week Regional training The project "Trusted flaggers for a safe Cyber Ecosystem Against Violent Extremism" is finalized The project "Trusted flaggers for a safe Cyber Ecosystem Against Violent Extremism" is finalized	 CYBER SECURITY NEWS BULLETIN October 2023 Content: National Authority for Electronic Certification and Cyber Security organizes preparatory training together with the Albanian National SOC Over 17,000 WordPress websites compromised by Balada Injector Google - Patching Alert National Authority for Electronic Certification and Cyber Security organizes preparatory training together with the Albanian National SOC Over 17,000 WordPress websites compromised by Balada Injector Google Chrome - patching alert	 CYBER SECURITY NEWS BULLETIN November 2023 Content: "Cyber Security Policy and Crisis Management" for the Transport and Energy Sectors. Capacity building, essential for the protection of critical and important information infrastructures "Cyber Security Policy and Crisis Management" for the Transport and Energy Sectors. Capacity building, essential for the protection of critical and important information infrastructures

November 2023	December 2023	December 2023
 CYBER SECURITY NEWS BULLETIN November 2023 Content: GitHub adds security measures with the help of artificial intelligence Samsung data breach Cisco - patching alert GitHub adds security measures with the help of artificial intelligence Samsung data breach Cisco - patching alert	 CYBER SECURITY NEWS BULLETIN December 2023 Content: A decade of awareness for children's online safety "Cyber Security Policies and Crisis Management" for Independent Institutions, the water Sector, NAIS and the State Police. A decade of awareness for children's online safety "Cyber Security Policies and Crisis Management" for Independent Institutions, the water Sector, NAIS and the State Police.	 CYBER SECURITY NEWS BULLETIN December 2023 Content: Toyota - data breach Google - patching alert Microsoft warns that hackers are exploiting OAuth applications PATCHING ALERT Google - patching alert

V. DIRECTORATE OF CYBER SECURITY ANALYSIS

The mission of the Directorate of Cyber Security Analysis is the analysis of networks and information systems and the digital examination of various cyber threats, to ensure protection against cyber-attacks on Critical and Important Information Infrastructures.

Part of the directorate's mission is coordination and cooperation with Critical and Important Information Infrastructures and other sectors engaged in the management of cyber incidents, to increase cyber resilience and take additional corrective measures for a faster and more efficient response to cyber incidents or attacks.

Directorate of Cyber Security Analysis:

1. Sector of Malware analysis and digital examination
2. Sector of Open-source analysis
3. Sector of Cyber protection

SECTOR OF CYBER PROTECTION

- The cyber defense sector, in order to increase cyber security, during 2023, has successfully met the following objectives:
- Analysis of Indicators of Compromise (IOC), which are reports from Critical and Important Infrastructures, the monitoring team or from reports of various campaigns received through Threat Intel platforms. These analyzes have helped identify trends, patterns and potential cyber threats.
- Sharing information with Critical and Important Infrastructures about Indicators of Compromise in order to increase security and avoid possible incidents.
- Improvement of the incident response plan, drawing up "Playbooks" for the 11 categories of incidents according to ENISA.
- Setting up simulation facilities such as:
  - *Sandbox*, to analyze malicious files and understand more about the behavior of these files.
  - Mail Server for simulating *mail spoofing* to report cases where these vulnerabilities exist.
- Collaboration with the Purple Team for creating scenarios of possible attacks to train the monitoring team (SOC) or the security teams of Critical and Important Infrastructures to increase the level of knowledge about cyber security. The trainings are developed in the form of exercises such as TTX and Cyber Drill.
- Cooperation with the "Red Team" team, to carry out the security assessment on the critical and important infrastructures which were the plan of the "Red Team" for the year 2023.
- Drafting and distribution of reports with recommendations for attack campaigns identified through research, through Threat Intel platforms or for known vulnerabilities (KEV) according to CISA.
- Methodological support in cases of incidents with high impact, assisting in the restoration of services in a relatively short time.
- In-depth analysis of logs reported by the monitoring team and logs made available from infrastructures affected by cyber incidents. By further understanding the techniques that malicious actors have followed.
- Cooperation with the SOC monitoring team for obtaining any information on anomalies identified during log monitoring, in order to guarantee secure services in information and communication technology.
- Based on the data of the monitoring systems, the analysis of cyber risks affecting the assets of critical and important information infrastructures was carried out in order to identify and treat them in order to reduce the risk and achieve a mature level of cyber security.

SECTOR OF OPEN-SOURCE ANALYSIS

Pursuant to the functional tasks, the open-source analysis sector monitors the activities on the Dark Web, analyzes the risks from the Dark Web and open sources, and identifies the potential risks of malicious actors in critical and important information infrastructures.

To accomplish operational tasks, the open-source analysis sector uses OSINT tools and resources to conduct information gathering on the tactics, techniques, and procedures used by malicious actors.

In order to prevent potential incidents in critical and important information infrastructures, reports on:

Vulnerabilities and Security Updates (38 Reports):

- **Critical Vulnerabilities (14 Reports):** Including vulnerabilities in Microsoft Message Queuing Service, Dell Power Manager, Cloudflare WARP Client, etc.
- **Security Updates (24 Reports):** Updates for Google Chrome, Android OS, Cisco products, McAfee Safe Connect, and others.

Malware and Ransomware Campaigns (13 Reports):

- **Ransomware Campaigns (5 Reports):** Yashma, Monti, Farnetwork Ransomware-as-a-Service, and others.
- **Malware Variants and Attack Techniques (8 Reports):** NodeStealer 2.0, MetaStealer Malware, Xloader, and more.

Zero-Day Attacks and Vulnerabilities (12 Reports):

- **Zero-Day Attacks and Attack Techniques (6 Reports):** Inception Attack on AMD Zen CPU, Cisco VPN, Mozilla etc.
- **Zero-Day and Critical Vulnerabilities (6 Reports):** Software vulnerabilities in Cisco-NX-OS, SolarWinds ARM, and others.

Cooperation with Other Sectors

- Report on Techniques, Tactics and Procedures for Iranian groups.
- Report on Techniques, Tactics and Procedures for Russian groups.
- Reports on other groups operating in the Western Balkans Region.

Important disclosures also include sensitive data, which are coordinated case by case with the responsible authorities in the field, such as the State Police and the Commissioner for the right to information and the protection of personal data.

SECTOR OF MALWARE ANALYSIS AND DIGITAL EXAMINATION

In implementation of the functional tasks, the Malware Analysis and Digital Examination sector performs the analysis of malicious programs and the digital examination of cyber incidents, with the aim of mitigating the harmful effects on the affected networks and systems, taking measures to recover the damages caused as well as the prevention of other similar incidents in all networks and information infrastructures.

- Examined, identified and understood the nature of various cyber threats such as viruses, worms, bots, rootkits, and Trojans. It has also identified critical threats stemming from Zero-Day and Ransomware Attacks.
- Assisted in technical and methodical support on the attacks that occurred as well as carried out post-analysis technical reports for all the incidents that occurred, drawing conclusions, recommendations and specific measures to prevent similar incidents.
- All post-analysis technical reports on incidents, recommendatory and preventive measures are forwarded to critical and important information infrastructures in real time through secure communication channels.
- Responded with immediate technical assistance to security incidents that were reported to the Authority, aiding until their resolution and detailed post-incident analysis.
- Conducted continuous research on developments in the field of cyber security and recommended security updates in cases where vulnerabilities were found. There are more than 200 reports forwarded to critical and important information infrastructures only for the first 6 months of the year, this number has increased for the second 6 months. A good part of the reports was compiled with the help of international sources and partners.
- Collaborated closely with other teams of the institution to create a clear report of security problems in the infrastructures that were tested. It is worth noting that the sector has contributed to increasing the capacities of the national SOC by constantly conducting Tabletop Exercises and Cyber Drills for the SOC.
- Participated in readiness exercises such as purple team, tabletop exercises, cyber drills which trained the security teams of critical and important information infrastructures, independent institutions, universities, etc. Specifically, some of the conducted trainings are:

➢ TTX and Cyber Drill for the Energy and Transport Sector
➢ TTX and Cyber Drill for the Financial sector
➢ Online training with all infrastructures in Albania
➢ Training on process analysis in Windows and Linux operating systems during the attack period of December 2023

- Examined incidents that occurred in Critical and Important Infrastructures using Malware Analysis and Digital Forensics tools. Specifically, managed 49 reported cyber incidents, of which 12 were classified as high impact.

- Has made an important contribution to the preparation of legal and by-laws related to the Authority's field of activity. Accordingly, the sector contributed to the drafting of the Cyber Incident Procedure, the creation of Playbooks, the drafting of the Cyber Crisis Procedure, etc.
- It has taken quick and efficient measures to respond to detected vulnerabilities to prevent and manage potential cyber incidents.
- Produced periodic or ad-hoc reports of high quality on incidents, security threats and discovered vulnerabilities some of which are mentioned below:

- ➢ Report and analysis for a new campaign by APT34
- ➢ Report and analysis on an attack campaign against Amazon S3
- ➢ Report on an attack campaign by CharmingKItten
- ➢ Report and analysis on a campaign of attacks by Winter Vivern
- ➢ Report on a campaign of attacks by Chinese APT
- ➢ Report and analysis on a phishing campaign by Muddy Water
- ➢ Report on a campaign by APT29 targeting embassies.
- ➢ Report on a new Agent Racoon attack campaign
- ➢ Lockbit 3.0 Ransomware analysis and report
- ➢ Report on the Homeland Justice TTP
- ➢ Analysis and report on malware Training Course.Zip
- ➢ Analyzes on Russian groups
- ➢ Report and analysis on Russian APT DDoS attack

- Represented the Authority in international conferences and participated in working groups and meetings within the country and within the institution. Directed the national CSIRT in the cyber training "Cyber Coalition 2023" in NATO.
- It has successfully implemented the implementation of some of the most important platforms, which have significantly contributed to the improvement and efficiency of work processes
- It has enabled the establishment of a platform for data storage which uses, automating the process of manual search of hashes, IPs or URLs. This platform has helped in the creation of daily reports in excel format of the IOC stored by the National SOC, their preservation by creating a history, as well as the help of deeper analysis of attempted attacks on CII/III.
- Effectively coordinated communications with other law enforcement institutions to take emergency measures to prevent cyber incidents. During this process, it has reported a high number of malicious IPs, illegitimate domains and harmful websites.

VI. DIRECTORATE OF OPERATIONS CENTER-CSIRT

The Directorate of the Operational Center has as the object of its activity the provision of a high level of cyber security of networks and systems, through their monitoring and interaction, continuous simulations, with the aim of increasing cyber resilience and taking additional corrective measures, for a faster and more efficient response to incidents or attacks that may affect critical and important Information infrastructures.

The Directorate of the Operational Center (CSIRT) consists of the Director of the Directorate and the two sectors:

- Cyber Incident Monitoring and Response Sector (SOC 1 & SOC2);
- Cyber Incident Simulation Sector.

In fulfilling its activity, the Directorate of the Operational Center coordinates the monitoring, response, management and handling of cyber incidents in critical and important information infrastructures, with the aim of preventing cyber incidents in them and their protection, provides methodical assistance and support for responsible operators in the field of cyber security, as well as conducts various simulations of incidents and attacks in order to increase technical and operational capacities at national level.

SECTOR OF CYBER INCIDENT MONITORING AND RESPONSE (SOC1 & SOC2)

Pursuant to functional tasks, the cyber incident monitoring and response sector (SOC1 & SOC2) performs 24/7 monitoring of networks and information systems, manages and handles real-time possible cyber incidents in critical and important information infrastructures, preventing the services and information they administer from being affected.

The sector of cyber incidents monitoring and response (SOC1 & SOC2) coordinates the work of monitoring, response, management and treatment of cyber incidents that occurred in critical and important information infrastructures, after categorizing the incidents identified during monitoring.

The monitoring process of the National SOC is carried out through agent and agentless platforms. The monitored operators belong to the sectors of critical and important information infrastructures, in accordance with the legislation in force, specifically the Decision of the Council of Ministers No. 553, dated 15.7.2020, "On the approval of the list of critical information infrastructures and the list of important information infrastructures", (amended by VKM No. 761, dated 12.12.2022). In this context, the National SOC monitors a total of about 133 operators of information infrastructures at the national level.

For the fulfillment of functional tasks, the National SOC monitors public IPs and all system interfaces that have public access by analyzing them in dedicated systems that analyze information about:

a) Malicious activity from these IP/Servers (Systems) to other servers on the Internet.
b) Activity from the Internet to the IP/Servers (Systems) of the infrastructures.

In real time, the National SOC communicates any anomalies identified in the information infrastructures with the latter's contact points, providing help and methodical support to operators responsible in the field of cyber security for cases of vulnerabilities or anomalies found during the monitoring process which they do not need in-depth analysis. For all other reports or detections, the National SOC escalates the case to other teams for more in-depth analysis.

SECTOR OF CYBER INCIDENT SIMULATION

In implementation of functional tasks, the sector of cyber incident simulations performs various simulations of incidents and attacks to increase the cyber resilience of information infrastructures and their technical and operational capacities.

The simulation of cyber-attacks is carried out based on the NAECCS Security Measures Control calendar, as well as upon official request from the infrastructure. Before performing the cyber-attack simulation, the "Rules of Engagement and Purpose of Work" are sent to the infrastructure, which contains the rules and the way to be scanned.

The infrastructure can choose if it wants only, Vulnerability Scanning or Attack Simulation and Email Phishing.

Also, before starting the control process at the operators of critical and important information infrastructures, the sector preliminarily performs an assessment of possible vulnerabilities for the IP addresses made available by the information infrastructures themselves, using various scanning sources, which help in the identification and treatment of problems.

For the year 2023, a total of ***27 Vulnerability Assessments*** were carried out for operators of critical and important information infrastructures defined in DCM No. 553, dated 15.7.2020 "On the approval of the list of critical information infrastructures and the list of important information infrastructures", as amended.

After completing the vulnerability assessment process, a report with relevant findings is drawn up, which includes:

1. The results of the scanning process for available IPs and the duration of this process.
2. Assessment of the level of risk that may have an impact on critical or important information systems:

- Info risk level **(0)**
- Low risk level **(0.1 – 3.9)**
- Medium risk level **(4.0 – 6.9)**
- High risk level **(7.0 – 8.9)**
- Critical risk level **(9.0 – 10.0)**

For the identified vulnerabilities, the level of risk, the description of the vulnerabilities and the way in which their mitigation can be carried out is determined. Recommendations based on the findings of the scanning process. These results cannot be considered as a final measure of safety for critical and important infrastructures.

Taking the proposed solutions into consideration in the mitigation process helps to reduce the level of risk to the infrastructure. NAECCS recommends applying all necessary updates based on the mitigation process section to each of the vulnerabilities and considering recommendations for all additional findings.

VII. DIRECTORATE OF FINANCE AND SUPPORT SERVICES

The Directorate of Finance and Support Services has two sectors in its structure:

- Sector of Finance
- Sector of Human Resources and Support Services

The purpose of the directorate is to implement the rules and laws of human resources management, financial management and control in the process of using budget funds, follow-up and drafting of budget requests, activity accounting and drafting of annual accounts.

Its objective is to guarantee the use of public funds, through the preliminary control of the compatibility of economic operations with the plan and legislation in force.

SECTOR OF FINANCE

Pursuant to Law No. 84/2022, "On the budget of 2023", Instruction of the Minister of Finance No. 9, dated 20.02.2018, "On standard procedures for the implementation of the budget" amended, Instruction of the Ministry of Finance No. .7 dated 28.2.2018, "On the standard procedures for the preparation of the PBA" as well as the Instruction of the Minister of Finance No. 22, dated 07.07.2023, "On the preparation of the Medium-Term Budget Program 2024-2026", National Authority on Electronic Certification and Cyber Security administers and manages the funds made available by the State Budget for 2023.

For the National Authority on Electronic Certification and Cybersecurity, the budget allocated for 2023 is 533,369 thousand ALL, of which 229,369 thousand ALL are Current Expenditures and 304,000 thousand ALL Capital Expenditures with internal financing as follows:
The plan of total expenses (in Lek) according to budget items is:

No.	Designation of Budget items	Plan of 2023
600	Wages	113,897,050
601	Social insurance	15,202,000
602	Other Goods and Services	99,894,000
603	Subsidies	
604	Domestic Current Transfers	
605	Foreign Current Transfers	170,000
606	Trans for Budget. Fam & Individual	206,000
231	Capital expenditures	304,000,000
TOTAL		**533,369,050**

[redacted]

Designation of Expenses	Initial Budget January - December 2023	Revised Budget January - December 2023	Budget January - December 2023	Fact January - December 2023	%
Current Expenses	238,302,000	229,369,050	229,369,050	137,022,888	59.7%
Internal capital	304,000,000	304,000,000	304,000,000	10,754,674	3.5%
Total Expenses	**542,302,000**	**533,369,050**	**533,369,050**	**147,777,562**	

SECTOR OF HUMAN RESOURCES AND SUPPORT SERVICES

Following the fulfillment of the mission of the Human Resources and Support Services Sector, for the management of human resources and the support services of NAECCS, the following have been carried out:

- Approval of job descriptions according to the structures approved by Prime Minister's Order No. 32, dated 16.03.2023 and No. 233 dated 20.12.2023.
- The reappointment of the current employees of NAECCS, in the new work positions, according to the structure approved by Prime Minister's Order No. 32, dated 16.03.2023, (20 employees and 2 trainee specialists with position outside the structure, within the framework of the National Program of Work Practices) and the structure approved by Prime Minister's Order No. 233 dated 20.12.2023, (48 employees and 1 trainee specialist with a position outside the structure, within the National Program of Work Practices);
- Approval of the new individual labor contract and signing of contracts with existing employees and new employees of NAECCS. (After the review of the current contract and the relevant changes, individual labor contracts were concluded, according to the approved structures);
- The procedure of recruiting new employees for vacant positions, throughout the year;
- Organization of work, assistance and cooperation with sectors for the realization of employee performance evaluation;
- Control of the correct implementation of the rules of ethics and discipline at work and the identification of problems according to the Internal Regulation in force;
- Management of human resources related to content and administrative procedures;
- Management of internal services of the institution, as well as management of archive/protocol activity, administration of the movement of correspondence inside and outside the institution and other support services.

Referred to Order No. 32 dated 16.03.2023 of the Prime Minister "On the approval of the structure and organization of the National Authority on Electronic Certification and Cyber Security", the structure of NAECCS has 85 employees and consists of 5 directors:

- **Directorate of Certification, Policies and Legal Affairs** (2 sectors).
- **Directorate of Cyber Security Governance, Control and Strategic Development** (3 sectors).
- **Directorate of Cyber Security Analysis** (3 sectors).
- **Directorate of the Operational Center – CSIRT** (2 sectors).
- **Directorate of Finance and Support Services** (2 sectors).

Referred to Order No. 233, dated 20.12.2023, "For the approval of the structure and organization of the National Authority on Electronic Certification and Cybersecurity", the structure of NAECCS was reorganized into 6 directorates:

- **Directorate of Certification, Policies and Cyber Security Legislation (2 sectors).**
- **Directorate of International Coordination Projects and Strategic Development of Cyber Security (2 sectors).**
- **Directorate of Monitoring and Incident Response, SOC C-SIRT Operational Center (2 sectors).**
- **Directorate of Cyber Security Analysis (2 sectors).**
- **Directorate of Compliance Analysis, Risk and Control of Cyber Security Measures (2 sectors).**
- **Directorate of Finance and Support Services (2 sectors).**

After the filling of the work positions, by the existing employees, there was a need to fill the vacant positions, according to the relevant directorates, a procedure which continued throughout the year. Referring to the above, to fill the vacancies of NAECCS, 19 internal orders were issued for recruitment announcements, for vacant positions, during the year 2023.
The plan of employee training and participation in various activities inside and outside the country was maintained and updated throughout the year 2023:

• Training abroad	47
• In-house training	14
• Reports/Conferences/Activities	20