

CROATIAN PARLIAMENT

1912

Pursuant to Article 88 of the Constitution of the Republic of Croatia, I hereby pass the

DECISION

PROMULGATING THE SECURITY AND INTELLIGENCE SYSTEM ACT OF THE REPUBLIC OF CROATIA

I hereby promulgate the Security and intelligence System Act of the Republic of Croatia, enacted by the Croatian Parliament at its session on 30 June 2006.

Class: 011-01/06-01/26

Reg. No: 71-05-03/1-06-2

Zagreb, 5 July 2006

The President of the Republic of Croatia
Stjepan Mesić, m.p.

SECURITY AND INTELLIGENCE SYSTEM ACT OF THE REPUBLIC OF CROATIA

I BASIC PROVISIONS

Article 1

(1) This Act establishes, for the purpose of systematic gathering, analysis, processing and evaluation of information relevant for the national security, with the aim of detecting and preventing activities, by individuals or groups, directed against the viability, independence, integrity and sovereignty of the Republic of Croatia, aiming at the violent overthrow of the state authority structures; threatening to violate human rights and basic freedoms established by the Constitution and the legislation of the Republic of Croatia, and to endanger the fundamentals of the economic system of the Republic of Croatia, required for making decisions relevant for successful achievement of national interests in the field of national security, the following security–intelligence agencies:

- Security and intelligence Agency (hereinafter: SOA),
- Military Security and intelligence Agency (hereinafter: VSOA).

(2) Facilitating cooperation between the President of the Republic of Croatia (hereinafter: the President of the Republic) and the Government of the Republic of Croatia (hereinafter: the Government), through provision of guidance for the work of security and intelligence agencies, shall be within the competence of the National Security Council, whereas the Council for the Coordination of Security and intelligence Agencies shall be responsible for the operational coordination of the work of security and intelligence agencies.

Article 2

(1) Security and intelligence agencies shall perform the functions from their respective scope of work pursuant to: the National Security Strategy, Defence Strategy, Annual guidelines for the work of security and intelligence agencies, laws, requests submitted by certain legally authorised state authorities, or requests by the users of work results produced by security and intelligence agencies.

(2) Security and intelligence agencies shall perform the functions from their scope of work in accordance with the Constitution of the Republic of Croatia, laws and other rules and regulations.

(3) The work of security and intelligence agencies shall be subject to the oversight by the Croatian Parliament, the President of the Republic, the Government, the Office of the National Security Council (hereinafter: UVNS) and the Council for the Civilian Oversight of Security and intelligence Agencies.

II NATIONAL SECURITY COUNCIL, COUNCIL FOR THE COORDINATION OF SECURITY AND INTELLIGENCE AGENCIES, OFFICE OF THE NATIONAL SECURITY COUNCIL, INFORMATION SYSTEMS SECURITY BUREAU, OPERATIONAL AND TECHNICAL CENTRE FOR TELECOMMUNICATIONS SURVEILLANCE

National Security Council

Article 3

(1) The National Security Council shall:

- examine and evaluate the intelligence and security threats and risks, examine matters from the scope of work of ministries and other state authorities related to national security, and adopt guidelines and conclusions on how to protect and accomplish the national security interests,
- examine matters from the scope of work of security and intelligence agencies, and establish ways for the effectuation of cooperation between the President of the Republic and the Government in directing the work of security and intelligence agencies, and approve cooperation between the agencies and counterpart foreign services,
- define Annual guidelines for the work of security and intelligence agencies, and adopt other decisions, by means of which, the President of the Republic and the Government shall direct the work of security and intelligence agencies and other entities of the security and intelligence system,
- define measures to be undertaken by the President of the Republic and the Government regarding the results of the oversight of work of security and intelligence agencies and other entities of the security and intelligence system,
- propose the resources required for the functioning of security and intelligence agencies and other entities of the security and intelligence system, which are to be secured from the state budget,
- examine other matters related to the functioning and management of security and intelligence agencies and other entities of the security and intelligence system.

(2) The term 'entities of the security and intelligence system' includes state authorities which, within the meaning of this Act, participate in the protection of the national security of the Republic of Croatia.

Article 4

(1) The National Security Council shall be composed of: the President of the Republic, the President of the Government, Member of the Government responsible for national security, the Minister of Foreign Affairs and European Integration, the Minister of Justice, National Security Advisor to the President of the Republic, the Chief of the General Staff of the Armed Forces of the Republic of Croatia (hereinafter: the Armed Forces), the Director of SOA, the Director of VSOA, and the Head of UVNS.

(2) The President of the Croatian Parliament shall take part in the work of the National Security Council.

(3) Meetings of the National Security Council shall be jointly convened and matters to be discussed and decided shall be jointly determined by the President of the Republic and the President of the Government. The meetings of the National Security Council shall be chaired by the President of the Republic, and the decisions thereof shall be co-signed by the President of the Republic and the President of the Government.

(4) In times of war or immediate threat against the viability, independence, unity and territorial integrity of the Republic of Croatia, the Chairperson of the Parliamentary Committee competent for national security, the Minister of Finance and the Minister of Economy shall also participate in the work of the National Security Council.

(5) The National Security Council may also invite other persons to participate in its meetings when general state of national security in the Republic of Croatia, particularly the state of national security in the fields of defence and domestic politics, the field of protection of human rights and basic freedoms are discussed, and in situations of large-scale natural and technological disasters, or when discussing the draft proposal of the National Security Strategy.

(6) The issues relevant for the functioning of the National Security Council shall be regulated by the Rules of Procedure.

Council for the Coordination of Security and intelligence Agencies

Article 5

(1) The Council for the Coordination of Security and intelligence Agencies shall implement the decisions of the President of the Republic and the President of the Government concerning the directing of the work of security and intelligence agencies, shall elaborate the decisions of the National Security Council regarding the work of security and intelligence agencies and other entities of the security and intelligence system, shall operationally coordinate the work of security and intelligence agencies and other entities of the security and intelligence system, shall give opinions on the cooperation with counterpart services in other countries, shall submit proposals to the National Security Council, and shall take other measures with the view of improving the effectiveness and the quality of work of security and intelligence agencies.

(2) The Council for the Coordination of Security and intelligence Agencies shall be composed of the Member of the Government responsible for national security, as the Chairperson of the Council for the Coordination of Security and intelligence Agencies; the National Security Advisor to the President of the Republic, as Deputy Chairperson; the Directors of security and intelligence agencies and the Head of UVNS. The meetings of the Council for the Coordination of Security and intelligence Agencies shall be convened, and the agenda items to be discussed and decided, shall be jointly determined by the Chairperson of the Council for the Coordination of Security and intelligence Agencies and the Deputy Chairperson. The meetings of the Council for the Coordination of Security and intelligence Agencies shall be chaired by the Chairperson of the Council for the Coordination of Security and intelligence Agencies, while the decisions shall be co-signed by the Chairperson of the Council for the Coordination of Security and intelligence Service and the Deputy Chairperson. The agenda items for the discussions may also be proposed by the Directors of security and intelligence agencies and by the Head of UVNS.

(3) When necessary and upon the invitation by the Chairperson of the Council for the Coordination of Security and intelligence Agencies, other persons may also participate in the meetings of the Council for the Coordination of Security and intelligence Agencies, in particular: Chief State Attorney, Director of USKOK, Director of Police, Director of Customs, Director of Financial Police, Director of Anti-Money Laundering Office, the representative of the Ministry of Foreign Affairs and European Integration responsible for security matters, Director of the National Protection and Rescue Directorate, and the top officials of other adequate inspection and oversight authorities.

(4) The meetings of the Council for the Coordination of Security and intelligence Agencies shall be convened at least once a month, but may also be convened when necessary or at the proposal of the standing members of the Council for the Coordination of Security and intelligence Agencies, referred to in paragraph 2 of this Article.

(5) The Council for the Coordination of Security and intelligence Agencies shall regulate the issues relevant for its own functioning by the Rules of Procedure

Office of the National Security Council (UVNS)

Article 6

(1) UVNS shall perform expert and administrative functions for the National Security Council and the Council for the Coordination of Security and intelligence Agencies, shall perform functions which facilitate the National Security Council to analyse the reports of security and intelligence agencies and to evaluate the fulfilment of the objectives set for security and intelligence agencies, to evaluate the implementation of the decisions of the President of the Republic and the President of the Government on directing the work of security and intelligence agencies, and the functions facilitating the President of the Republic and the President of the Government to supervise the performance of security and intelligence agencies.

(2) UVNS shall integrate the reports and the information received from security and intelligence agencies, draft periodic reports covering different areas of security and intelligence activity, and analyse and evaluate the security and intelligence information relevant for the national security of the Republic of Croatia and essential for the execution of constitutional and legal powers of the President of the Republic and the President of the Government.

(3) At the request of the President of the Republic and the President of the Government UVNS shall cooperate with security and intelligence agencies in drafting the strategic assessments and evaluations of the

security-related developments relevant for the national security of the Republic of Croatia.

Article 7

(1) UVNS is the central state authority responsible for determining and implementation of the activities related to the application of information security measures and the adoption of information security standards in state authorities in the Republic of Croatia, and for the coordination of activities with respect to the application of the information security measures and standards in the exchange of classified information between the Republic of Croatia and foreign countries and organisations.

(2) Within the meaning of this Act, the term “classified information” means any information classified, by the competent state authority and in accordance with the legislation regulating data secrecy protection, as secret.

(3) Information security measures and standards shall be applied within the framework of information security areas: personnel security, physical security, security of information, INFOSEC, and industrial security, and shall be stipulated by the separate Act regulating the information security area.

(4) The Central Registry for the reception, storage and distribution of information and documents exchanged with foreign countries and organisations (hereinafter: Central Registry) shall operate within the structure of UVNS.

(5) For the performance of functions of the Central Registry Sub-registries of the Central Registry shall be established within state authorities. Provisions of this Act, regulating the status, rights, obligations and responsibilities, and the manner of determining salaries of the employees of UVNS, shall also apply to the employees of the Sub-registries of the Central Registry.

(6) UVNS shall issue Personnel Security Clearances (Certificates) on conducted security vetting for the persons who, within the performance of their duties, have classified data access.

(7) Certificates referred to in paragraph 6 of this Article shall also be issued for legal persons performing functions relevant for the national security of the Republic of Croatia, and at the request of foreign countries and organisations.

Article 8

UVNS shall submit its annual reports and the special reports on its work, annual and special reports on the performance of the professional oversight of the work of security and intelligence agencies and the Operational and Technical Centre for Telecommunications Surveillance (hereinafter: OTC) to the President of the Republic and the President of the Government. UVNS shall submit annual reports on the oversight inspections conducted to ensure the respect of rights of citizens guaranteed by the Constitution of the Republic of Croatia both to the President of the Croatian Parliament and the Parliamentary Committee competent for national security, while special reports on professional oversight shall be submitted to the President of the Croatian Parliament and the Parliamentary Committee competent for national security, when the oversight is conducted at their request.

Article 9

UVNS shall not perform functions which, pursuant to the provisions of this Act, pertain to the scope of work of security and intelligence agencies and shall not apply, in the performance of its functions, measures which the security and intelligence agencies are authorised to use.

Article 10

(1) The work of UVNS shall be managed by the Head of Office, appointed to and relieved of his/her duty by a decision co-signed by the President of the Republic and the President of the Government. The Head of UVNS shall be appointed for a four-year term. No person may be appointed to the position of the Head of UVNS for more than two consecutive terms.

(2) The Head of UVNS may be relieved of his/her duty before the expiry of the mandate: at his/her own request; if he/she becomes permanently incapacitated for the performance thereof; he/she does not ensure the performance of the functions from the scope of activity of UVNS; due to the violation of the Constitution, laws and other rules and regulations, due to abuse or exceeding of authority, the violation of classified data secrecy, and the pronouncing of the final verdict for criminal offence which renders him/her unworthy of the position.

(3) The Head of UVNS is a state official within the meaning of the Act on State Officials' Rights and

Obligations.

Article 11

The internal organisation of UVNS, functions of its structural units, and the approximate number of the personnel required for the performance of functions, the form and content of the official identification card and official badge, and the authorisation to use them, as well as other matters relevant for the operation of UVNS, shall be regulated by the Regulation adopted by the Government, with the prior consent of the President of the Republic. The modus operandi, the required number of employees with their respective job descriptions and necessary requirements for the performance thereof, their powers and responsibilities, rights resulting from the employment, and other matters relevant for the functioning of UVNS, shall be regulated by the Ordinance on internal order, to be passed by the Head of UVNS, with the approval of the National Security Council.

Article 12

To the Head and the employees of UVNS appropriate provisions of this Act, regulating the status, rights, obligations and responsibilities, and the manner of determining salaries of officials and employees of security and intelligence agencies (Title VII) shall apply, whereas, to matters not regulated by this Act, the Act on Civil Servants, and the Act on State Officials' Rights and Obligations shall apply.

Information Systems Security Bureau

Article 13

Under this Act, the Information Systems Security Bureau (hereinafter: ZSIS) is established as the central state authority for the performance of functions in technical areas within the field of information security in state authorities of the Republic of Croatia.

Article 14

(1) ZSIS shall perform functions in the fields of information systems and networks security, of security accreditations of information systems and networks in state authorities, handling of crypto materials used in classified data exchange between the state authorities of the Republic of Croatia and foreign countries and organisations, and coordination of the prevention and removal of problems related to the security of computer networks in state authorities.

(2) ZSIS shall also conduct works of research, development and testing of technologies intended for the protection of classified data, and shall issue certificates for the use thereof.

(3) Accreditations referred to in paragraph 1 and certificates referred to in paragraph 2 of this Article shall be issued by ZSIS pursuant to the agreements on the exchange of classified information (Security Agreements) between the Republic of Croatia and foreign countries and organisations.

Article 15

(1) The work of ZSIS shall be managed by the Director who is appointed to, and relieved from his/her position by the Government decision, at the proposal of the Council for the Coordination of Security and intelligence Agencies. The Director shall be appointed for a four year period, and the same person may be reappointed.

(2) The Head of ZSIS may be relieved of his/her duty before the expiry of the mandate: at his/her own request; if he/she becomes permanently incapacitated for the performance of his/her duties; if he/she does not ensure the performance of the functions from the scope of activity of ZSIS; due to the violation of the Constitution, laws and other rules and regulations, due to abuse or exceeding of authority, the violation of classified data secrecy; if he/she is pronounced the final verdict for criminal offence which renders him/her unworthy of the position.

(3) The Director of ZSIS shall report on his/her work to the Head of UVNS.

(4) With the approval of the Government, the Director of ZSIS shall appoint his/her own Deputy.

Article 16

(1) Internal organisation of ZSIS, functions of its structural units, and the approximate number of personnel required for the performance of the functions thereof shall be regulated by the Regulation on internal order to be adopted by the Government at the proposal of the Director of ZSIS with the consent of the Council for

the Coordination of Security and intelligence Agencies.

(2) The modus operandi, the required number of employees with their respective job descriptions and necessary requirements for the performance thereof, their powers and responsibilities, rights resulting from the employment, and other matters relevant for the functioning of ZSIS not regulated by the Regulation referred to in paragraph 1 of this Article, shall be regulated by the Ordinance on internal order, to be passed by the Director of ZSIS, with the approval of the Government.

Article 17

To the Head and the employees of ZSIS appropriate provisions of this Act, regulating the status, rights, obligations and responsibilities, and the manner of determining salaries of the officials and employees of security and intelligence agencies (Title VII) shall apply, whereas to matters not regulated by this Act, provisions of the Act on Civil Servants and the Act on State Officials' Rights and Obligations shall apply.

Operational and Technical Centre for Telecommunications Surveillance (OTC)

Article 18

(1) For the purpose of activation and management of the measures of secret surveillance of telecommunications services, activities and traffic, and in order to enable the operational-technical coordination between the legal and natural persons operating public telecommunications networks and providing public telecommunications services and access services in the Republic of Croatia, and the bodies authorised to apply measures of secret surveillance of telecommunications pursuant to this Act and the Criminal Procedure Act, the Operational and Technical Centre for Telecommunications Surveillance shall be established (hereinafter: OTC).

(2) In cooperation with the bodies authorised for the application of measures of secret telecommunications surveillance in accordance with this Act and the Criminal Procedure Act, OTC is authorised to supervise the work of telecommunications services providers, i.e. their fulfilment of the obligations stipulated by this Act.

(3) OTC shall, for the purpose of security and intelligence agencies and monitoring bodies, conduct the activation and management of the measures of secret surveillance of telecommunications services, activities and traffic, by means of appropriate technical interface.

Article 19

(1) Legal and natural persons referred to in Article 18, paragraph 1 of this Act, shall ensure and maintain, at their own expense, the function of secret surveillance of telecommunications services, activities and traffic referred to in Article 33, paragraph 3, item 1 of this Act, as well as maintain the communication lines towards the OTC. For the purpose of effectuation of secret surveillance, the appropriate technical equipment and program support shall be incorporated into the telecommunications system of the legal and natural persons referred to in Article 18, paragraph 1 of this Act.

(2) The legal and natural persons referred to in Article 18, paragraph 1 of this Act shall ensure, for OTC, the conditions for permanent and direct access to facilities and technical equipment, and the conditions for autonomous application of the measures referred to in Article 33, paragraph 3, item 1 of this Act, by means of appropriate technical interfaces.

(3) The Ministry of Defence and the Armed Forces of the Republic of Croatia, and state authorities that have their own telecommunications networks shall facilitate to the OTC to apply measures of secret information gathering and ensure the conditions for direct access to facilities and technical equipment, and conditions for the autonomous application of measures.

(4) Legal and natural persons referred to in Article 18, paragraph 1 of this Act must, in cooperation with OTC, ensure autonomous and exclusive access to data on activated measures. The competent supervisory and investigative bodies shall also be provided access to data on activated measures, within the framework of their authorities and procedures stipulated by law.

(5) Legal and natural persons referred to in Article 18, paragraph 1 of this Act shall keep the secrecy of data on the users of services in telecommunications transactions for one year.

(6) Legal and natural persons referred to in Article 18, paragraph 1 of this Act shall provide, at the request of OTC, information regarding all means of communication that have appeared at certain geographical, physical or logical location, regardless of the telecommunications (in)activity thereof, within the period of previous 48 hours.

Article 20

(1) Obligations stipulated by this Act referring to legal and natural persons operating public telecommunications network and providing public telecommunications and access services related to the function of secret surveillance shall be regulated by the Government Regulation on obligations of legal and natural persons in the field of national security in the telecommunications area, to be adopted upon the proposal of the Council for the Coordination of Security and intelligence Agencies.

(2) Obligations of the Ministry of Defence and the Croatian Armed Forces stipulated by this Act, related to the function of secret surveillance, if they operate their own telecommunications networks, shall be stipulated by the Minister of Defence upon the proposal of the Director of VSOA.

(3) SOA and VSOA, in cooperation with other bodies authorised for the application of measures of secret surveillance of telecommunications pursuant to the Criminal Procedure Act, with the approval of the Council for the Coordination of Security and intelligence Agencies, shall adopt the rules and regulations regarding the technical requirements, the development of the appropriate technical equipment and program support, issues of technical interfaces, and other matters relevant for the activation and the application of the measures of secret surveillance of telecommunications.

Article 21

(1) The work of OTC shall be managed by the Director who is appointed to, and relieved from the position by the Government Decision, upon the proposal of the Council for the Coordination of Security and intelligence Agencies. The Director shall be appointed for a four year period, and the same person may be reappointed.

(2) The Director of OTC may be relieved of his/her duty: at his/her own request; if he/she becomes permanently incapacitated for the performance of duties; if he/she does not ensure the performance of the functions from the scope of activity of OTC; due to the violation of the Constitution, laws and other regulations, due to abuse or exceeding of his/her authority, the violation of classified data secrecy, and the pronouncing of the final verdict for criminal offence which renders him/her unworthy of the position.

(3) The Director of OTC shall report of his/her work to the UVNS.

Article 22

(1) The internal organisation of OTC, the functions of its structural units, and the approximate number of the personnel required for the performance of the functions shall be regulated by the Regulation on internal organisation to be adopted by the Government upon the proposal of the Council for the Coordination of Security and intelligence Agencies.

(2) The modus operandi, the required number of employees with their respective job descriptions and necessary requirements for the performance thereof, their powers and responsibilities, rights resulting from employment, and other matters relevant for the functioning of OTC, that are not regulated by this Act or the Regulation referred to in paragraph 1 of this Article, shall be regulated by the Ordinance on internal order, to be adopted by the Director of OTC, with the approval of the Council for the Coordination of Security and intelligence Agencies.

(3) To the Head and the employees of OTC appropriate provisions of this Act, regulating the status, rights, obligations and responsibilities, and the manner of determining salaries of the officials and employees of security and intelligence agencies (Title VII) shall apply, whereas to matters not regulated by this Act, the provisions of the Act on Civil Servants and the Act on State Officials' Rights and Obligations shall apply.

III SECURITY AND INTELLIGENCE AGENCIES

Security and intelligence Agency (SOA)

Article 23

(1) On the territory of the Republic of Croatia the functioning of SOA is directed against the activities or actions aimed at threatening the Constitutional order, safety of state authorities, citizens and national interests, by means of:

- terrorist acts and other forms of organized violence;
- the intelligence activity of foreign intelligence services, organisations and individuals;
- the extremist organizations and activities of groups and individuals;

- endangering the safety of top state officials and protected facilities and areas;
- organised and economic crime;
- unauthorised access to protected information and communication systems of state authorities;
- disclosure of classified information by state officials or the employees of state authorities, scientific institutions and legal persons with public authority,
- other activities aimed at threatening national security.

(2) SOA shall collect, analyze, process and evaluate the political, economic, scientific/technological and security-related information concerning foreign countries, organisations, political and economic alliances, groups and persons, especially those showing intentions, potential, concealed plans and clandestine activities directed against the national security, or other information relevant for the national security of the Republic of Croatia.

Military Security and intelligence Agency (VSOA)

Article 24

(1) VSOA is a structural unit of the Ministry of Defence intended to provide planning and implementing support to the Ministry of Defence and the Armed Forces in their performance of duties in the area of protection of viability, sovereignty, independence and territorial integrity of the Republic of Croatia.

(2) VSOA shall collect, analyze, process and assess information on armies and defence systems of other countries, on external pressures which might influence the defence security, and on the international activities directed against the defence security of the country.

(3) On the territory of the Republic of Croatia VSOA shall collect, analyze, process and evaluate information on the intentions, potential and plans for actions by certain persons, groups and organisations in the country, the objective of which is to threaten the defence capabilities of the country, and shall take measures aimed at identifying, monitoring and combating such activities.

IV FUNCTIONS AND AUTHORITY OF SECURITY AND INTELLIGENCE AGENCIES

Information Gathering

Article 25

Security and intelligence agencies, within their respective scope of activities, shall gather information from publicly available sources, by communication with citizens, by requesting data from state authorities, bodies of local and regional self-government, legal persons, including access to registries and databases and the official documentation, and by applying secret procedures and measures.

Article 26

(1) In the performance of functions referred to in Article 24, paragraph 3 of this Act, VSOA shall apply measures and procedures stipulated by this Act only against the employees or members of the Ministry of Defence and the Armed Forces.

(2) Where, acting pursuant to the provisions of paragraph 1 of this Article, VSOA learns and assesses that the measures and procedures stipulated by this Act should also be applied against other persons, it shall immediately inform SOA thereof, and they shall jointly decide on further actions.

Article 27

(1) When officers of security and intelligence agencies gather information by communication with citizens and at the same time make formal inquiries or request other forms of assistance, they shall identify themselves by presenting their official identification cards and badges.

(2) Interviews in the official premises of security and intelligence agencies may be conducted with citizens only with their expressly stated consent. Such interviews shall be recorded by technical means and, by signing the minutes citizens shall confirm the voluntary nature of the interviews and verify the authenticity and integrity of the recorded conversations.

(3) Minutes and recordings of the interviews referred to in paragraph 2 of this Article shall be kept in the competent structural units of security and intelligence agencies, and shall be available to the competent judiciary or oversight bodies.

(4) Where there are grounds to assume that a citizen, who did not agree to the interview with officers of security and intelligence agencies, possesses information relevant for the national security, the security and intelligence agency shall request the Ministry of Interior, or the Police, to conduct an informative interview with the citizen, in accordance with the procedure stipulated by a separate Act. If such an informative interview takes place, the officer of the security and intelligence agency shall also participate in it.

Article 28

(1) In case there is reasonable doubt that foreign intelligence or security services, individuals or groups are preparing or taking actions which might threaten the defence security of the country, VSOA shall summon employees or members of the Ministry of Defence and the Armed Forces for informative talks, and shall have access to documentation and data kept by the Ministry of Defence and the Armed Forces.

(2) Employees and members of the Ministry of Defence and the Armed Forces shall respond to the summons referred to in paragraph 1 of this Article.

Article 29

(1) Security and intelligence agencies may gather information by the assistance of secret collaborators. Forcing anyone to become a secret collaborator is not permitted.

(2) Security and intelligence agencies shall protect the identity of persons registered as secret collaborators and, if necessary, ensure their physical safety and the safety of their families and their property.

(3) Security and intelligence agencies may contract life insurance policies for registered secret collaborators for the risks that can be expected with regards to the tasks performed for the agencies.

(4) A registered secret collaborator who is injured or falls ill while performing functions assigned to him/her by the security and intelligence agency, if he/she does not have any insurance on other grounds, is entitled, during medical treatment, to the same rights from medical insurance as if he/she were an employee of the security and intelligence agency, whereas in case of disablement caused by an injury or illness incurred or contracted during the performance of the functions assigned to him/her by the security and intelligence agency, he/she is entitled to the rights from the pension insurance equal to those of the employees of the security and intelligence agency.

(5) Exercising of the rights referred to in paragraph 4 of this Article shall be regulated in more details in the Rules of Procedure to be passed by the Directors of security and intelligence agencies.

(6) In cases of accidents occurring in relation to the performance of functions assigned by the security and intelligence agency, resulting in death of a registered secret collaborator, his/her family shall be entitled to the rights referred to in Article 81, paragraphs 2 and 3 of this Act.

Article 30

Officials and employees of state authorities and local (regional) self government bodies and of legal persons with public authority, as well as the employees or members of the Ministry of Defence and the Armed Forces, shall comply with the requests of security and intelligence agencies regarding the data available to them within their respective scope of activity.

Article 31

Officers of security and intelligence agencies may either have direct access into registers and databases or documentation after they have identified themselves with their official identification cards and badges, or have permanent access to computer databases, or otherwise established databases, through the use of appropriate interfaces as laid down by law.

Article 32

(1) State authorities, units of local (regional) self-government and legal persons, as well as the members of the Ministry of Defence and the Armed Forces may maintain records of all effectuated access to their respective databases, registers and documentation, which may include only numbers of badges or numbers of the official identification cards of the officers of security and intelligence agencies. Records of the numbers of badges or identity cards of the officers of security and intelligence agencies shall be kept

separate from other records.

(2) Officials and employees of the bodies referred to in paragraph 1 of this Article shall keep the secrecy of all knowledge disclosed to them on the matters of interest of security and intelligence agencies.

Article 33

(1) SOA may apply measures of secret information gathering, which temporarily restrict certain constitutional human rights and basic freedoms, against citizens. VSOA may apply measures of secret information gathering, which temporarily restrict certain constitutional human rights and basic freedoms, only against the employees or members of the Ministry of Defence and the Armed Forces.

(2) The measures of secret information gathering, which temporarily restrict certain constitutional human rights and basic freedoms, may be applied if the information cannot be obtained in any other way or the collection thereof is linked with disproportionate difficulties. In cases where choice between several different measures of secret information gathering is possible, the one less invasive to constitutionally protected human rights and basic freedoms shall be applied.

(3) Measures of secret information gathering include:

1. Secret surveillance of telecommunications services, activities and traffic:

- a) Secret surveillance of the communication content
- b) Secret surveillance of the telecommunications traffic data
- c) Secret surveillance of the location of the user
- d) Secret surveillance of international telecommunications.

2. Postal censorship,

3. Secret surveillance and technical recording of the interior of facilities, closed spaces and objects,

4. Secret surveillance and monitoring, with recording of images and photos of persons in open and public spaces,

5. Secret surveillance and monitoring, with audio recording of the content of communication between persons in open and public spaces,

6. Secret purchase of documents and objects.

Article 34

The Ministry of Defence and the Armed Forces, as well as legal and natural persons who perform functions of postal and other deliveries shall facilitate the security and intelligence agencies the implementation of measures of secret information gathering, and shall provide conditions for direct access to facilities and technical equipment, and conditions for the autonomous application of these measures.

Article 35

Officials, or other responsible persons and employees of legal persons, employees of state authorities, members of the Armed Forces and other natural persons who possess information concerning the application of measures of secret information gathering on the part of security and intelligence agencies under the provisions of Articles 33 and 34 of this Act, shall keep such information secret.

Article 36

(1) Measures of secret information gathering referred to in Article 33, paragraph 3 items 1 a), 2, 3 and 6 of this Act may only be applied based on a written justified warrant for the application thereof, issued by the judge of the Supreme Court of the Republic of Croatia. Judges authorised to issue written warrants for the application of secret information gathering measures shall be selected by the President of the Supreme Court of the Republic of Croatia. The written justified proposals for the application of secret information gathering measures shall be submitted by the Directors of security and intelligence agencies.

(2) As an exception to the provisions of paragraph 1 of this Article, if a delay in the application of secret information gathering measures would prevent the achievement of the intended objective, the application of the measures may begin on the basis of the order by the Director of security and intelligence agency, who shall immediately inform the competent judge of the Supreme Court of the Republic of Croatia thereof. The competent judge shall, within 24 hours from the beginning of the application of measures, decide whether to issue the warrant authorising the application of measures. If the competent judge does not issue, or refuses to issue a written warrant for the application of measures within 24 hours, the security and intelligence agencies shall terminate the application of measures and shall destroy the documents and media where the

information gathered during the application of measures has been recorded, shall draft a report thereon and submit it to the competent judge of the Supreme Court.

(3) When the competent judge of the Supreme Court does not, or refuses to, issue the warrant for the application of measures for secret information gathering, he/she shall inform UVNS about the reasons for the refusal.

(4) Proposals and warrants for the application of measures of secret information gathering shall include the indication of the specific measure to be applied, shall indicate the natural or legal person against whom the measure shall be applied, the reasons justifying the application, the intended purpose and duration of the measure. If the application of more than one measure is being proposed and allowed, the information regarding each measure shall be indicated. Proposals for the application and warrants for the application of measures of secret information gathering shall be classified. Officers and other persons taking part in the decision making process and in the application of measures shall keep the secrecy of all the information they have learned in the process.

Article 37

(1) The measures of secret information gathering referred to in Article 33, paragraph 3, items 1 a), 2 and 3 of this Act may last up to four months.

(2) In case where the extension of the measure or the application of additional measures against the same person is necessary, the decision on the approval of the warrant shall be made by a Council composed of three authorised judges of the Supreme Court.

(3) Prior to the approval of the warrant referred to in paragraph 2 of this Article, the Council of three authorised judges of the Supreme Court is authorised to request additional justifications and reasons from the Directors of security and intelligence agencies, and is also authorised to ask the opinion of UVNS on the professional foundation of the request with respect to the applied methods and the seriousness of security threats.

Article 38

(1) Application of the measures referred to in Article 33, paragraph 3, subparagraph 1, items b, c, d, and subparagraphs 4 and 6, shall be approved by a written and justified warrant issued by the Directors of security and intelligence agencies within their respective scope of activities.

(2) The Directors of security and intelligence agencies shall, on a monthly basis, report to UVNS about the issued warrants, while the reports on the measure referred to in Article 33, paragraph 3, subparagraph 6 of this Act shall be submitted to the Chief State Attorney as well.

Databases and the Use Thereof

Article 39

(1) Security and intelligence agencies shall establish and maintain databases and registers of personal data and other records of gathered information and documents with the data related to the scope of activity of security and intelligence agencies, and other records related to their respective functions and activities.

(2) Persons acquainted with the data contained in the records of security and intelligence agencies and in the documents related to such data shall keep the secrecy thereof.

Article 40

(1) Security and intelligence agencies shall inform the citizens, within 15 days upon their request in writing, if measures of secret information gathering have been applied against them, or if files with their personal data are kept, and upon their request shall allow them access to the said data.

(2) Documents inspected by the citizens shall not contain information on the employees of security and intelligence agencies, or any information on the sources of security and intelligence agencies, or on any third persons.

(3) Security and intelligence agencies are authorised not to act in accordance with the provisions of paragraph 1 of this Article if:

- the information would jeopardise the fulfilment of the agency tasks,
- the information could result in a threat to the security of another person,
- the information could result in consequences harmful for the national security and national interests of the

Republic of Croatia.

(4) As soon as the reasons for the implementation of provisions of paragraph 3, subparagraphs 1 and 2 of this Article cease to exist, the security and intelligence agencies shall act in accordance with the provisions of paragraph 1 of this Article. In cases referred to in paragraph 3, subparagraph 3 of this Article they need not act in accordance with the provisions of paragraph 1 of this Article before the expiry of a 10 year period following the date of the termination of the application of measures.

Article 41

(1) Documents containing information with no relevance to the purpose for which they have been gathered, shall be destroyed within 30 days in the presence of the competent commission and a report shall be drafted within the period of 30 days.

(2) Data, documents and information gathered in an illegal manner shall be destroyed within 30 days, and a report which has to be signed by the persons who witnessed the destruction of such data, documents and information shall be drafted within the period of 30 days.

(3) Data, documents and information that do not refer to the purpose for which they have been gathered, or which have been gathered by the work of security and intelligence agencies in an illegal manner in the past, shall be singled out, shall not be used and shall be destroyed within the period of 2 years from the date of entry into force of this Act.

Security Vetting and Counterintelligence Protection

Article 42

Security vetting shall be performed for the officials and employees of security and intelligence agencies, the Head and the employees of UVNS, the Directors and employees of ZSIS and OTC, the Chairperson and the members of the Council for the Civilian Oversight of Security and intelligence Agencies, and for other persons identified in the provisions of this Act and other Acts and Regulations of the Government of the Republic of Croatia within the framework of their appointment to duty or admission to service. Security vetting shall also be performed for the persons who are granted Croatian citizenship and for the foreigners in the Republic of Croatia whose residence is important for national security.

Article 43

When performing the functions of counterintelligence protection VSOA shall, in accordance with the provisions of this Act, perform security vetting of the employees or the members of the Ministry of Defence or the Armed Forces and of the persons who have either become or are about to become employees of the Ministry of Defence and the Armed Forces.

Article 44

Within the security vetting procedure, the person being vetted may be interviewed; other persons related to the vetted person may also be talked to; data contained in official databases maintained by other services, institutions and authorities may be used, and measures of secret data gathering may be applied, as well as the polygraph testing.

Article 45

Security vetting shall be conducted for Croatian and foreign natural and legal persons with whom security and intelligence agencies and other state authorities relevant for the national security intend to conclude contracts for the acquisition of goods or the provision of services which will provide natural or legal person with access to classified data or access to protected persons or facilities in a way that can influence the security of said persons or facilities.

Article 46

(1) VSOA shall participate in the counterintelligence protection and shall safeguard the security of protected employees or members, facilities and spaces of the Ministry of Defence and the Armed Forces, identified by the Minister of Defence; it also shall provide additional support by participating in the protection of other members, facilities and spaces of the Armed Forces, and it shall take part in the counterintelligence protection and shall safeguard the weapons and military equipment production intended for the Armed

Forces.

(2) VSOA shall take care of the counterintelligence security of employees, or members and facilities of the Ministry of Defence and the Armed Forces abroad and for that purpose may cooperate with the adequate structural unit of the Ministry of Foreign Affairs and European Integration responsible for security matters.

Article 47

(1) In the performance of the functions of counterintelligence protection of protected persons, facilities and institutions security and intelligence agencies shall develop, in their respective scope of work, security assessments of the potential security risks threatening the protected persons and facilities, shall conduct security vetting of persons with access to protected persons, facilities and objects, shall apply technical surveillance counter-measures in facilities and objects, and shall participate in the planning, implementation and oversight of technical and physical security measures.

(2) Protected persons, facilities and objects shall be identified, and the manner in which the measures referred to in paragraph 1 of this Article are to be implemented shall be defined by a separate Government Regulation and the Ordinance passed by the Minister of Defence for his/her scope of work.

Article 48

(1) Security and intelligence agencies, in their respective scope of work, shall apply technical surveillance counter-measures and conduct inspection of the facilities referred to in Article 47, paragraph 2 of this Act, shall supervise the construction/technical works, technical documentation of the facilities, installations, telecommunications and information equipment, and shall take part in the planning, implementation and oversight of technical and physical security measures used in the said facilities.

(2) Security and intelligence agencies shall conduct security vetting of the persons employed for jobs of physical and technical protection, technical and information maintenance in the facilities referred to in Article 47, paragraph 2 of this Act, and shall conduct security vetting of legal persons and their employees who take part in the works which can influence the technical surveillance counter-measures referred to in paragraph 1 of this Article.

(3) SOA shall safeguard the counterintelligence security of citizens and institutions of the Republic of Croatia abroad, and to that end it shall cooperate with the corresponding structural unit of the Ministry of Foreign Affairs and European Integration responsible for security matters.

(4) Security and intelligence agencies shall take part in counterintelligence protection and shall safeguard the security of their own employees, facilities and objects, and other persons, facilities and objects.

(5) Security and intelligence agencies shall, depending of the security threat assessments, also safeguard the security of former agency employees in case where such threats result from their previous work in security and intelligence agencies.

Article 49

In the performance of functions referred to in Article 48, paragraphs 4 and 5 of this Act the employees of security and intelligence agencies shall exercise the rights and powers in accordance with legal acts regulating the conduct with persons engaged in works of private protection of persons and property.

Article 50

In line with the specific interests and needs of SOA, a separate agreement on the cooperation between SOA and the Ministry of Interior of the Republic of Croatia (hereinafter referred to as: MoI RoC) shall regulate the form and the manner of cooperation between SOA and the Ministry of the Interior.

Article 51

(1) The information security functions performed by security and intelligence agencies include regular oversight of the organisation and the implementation of stipulated information security measures in state authorities, and reporting to competent state bodies on the status and effectiveness of stipulated information security standards in state authorities and on their possible improvements.

(2) Security and intelligence agencies shall perform functions of security vetting of natural and legal persons referred to in Article 7, paragraphs 3 and 6 of this Act.

(3) Functions referred to in paragraphs 1 and 2 of this Article shall be performed by SOA, except those within the Ministry of Defence and the Armed Forces, which shall be performed by VSOA.

(4) At the request of security and intelligence agencies UVNS and ZSIS shall provide access to information security data necessary to security and intelligence agencies in the performance of functions from their respective scope of duty.

Measures of Concealment

Article 52

Security and intelligence agencies may, when performing works from their respective scope of duty, implement measures of concealment of ownership of objects and legal persons, measures of concealment of true identity of their employees and other persons, measures concealing the purpose of data gathering and, when necessary, may use secret services of legal and natural persons, provided in return for compensation.

Article 53

Information on the measures referred to in Article 52 of this Act, and on the expenses of the implementation thereof, shall constitute a secret and shall be available only to the bodies and persons identified in the decision passed by the National Security Council at the proposal of the Chairperson of the Council for the Coordination of Security and intelligence Agencies.

Article 54

(1) The activity and material/financial operating of concealed legal persons shall be conducted in accordance with the regulations valid for that particular type of activity. No legal person financed directly from the state budget of the Republic of Croatia may be a concealed legal person. The concealed legal persons shall be established and maintained from the resources of security and intelligence agencies. Expenses incurred in such way shall be reported as security and intelligence budgetary expenses intended for special purposes.

(2) All assets owned by concealed legal persons shall be the property of the Republic of Croatia, and proceeds from such activity shall be used by security and intelligence agencies in the performance of their functions as funds intended for special purposes.

Reporting

Article 55

(1) All relevant information collected in their work and assessments of security situation shall be reported by security and intelligence agencies to the President of the Republic, the President of the Parliament, the President of the Government, and the Head of UVNS. VSOA shall deliver its reports to the Minister of Defence and, in case it refers to the Armed Forces, it shall also report to the Chief of the General Staff of the Armed Forces. Ministers and other state officials shall receive reports related to their respective area of responsibility.

(2) Annual reports on their work shall be submitted by security and intelligence agencies to the President of the Republic, the President of the Parliament, the Chairperson of the Parliamentary Committee competent for matters of national security, the President of the Government and the Head of UVNS and, at their request, security and intelligence agencies shall also provide special reports on the national security situation from their respective scope of activity.

Article 56

(1) Where the collected intelligence indicates that a criminal act which is prosecuted ex officio is being planned or committed, security and intelligence agencies shall notify State Attorney's Office thereon.

(2) The notification referred to in paragraph 1 of this Article may, by way of exception, include data regarding the manner in which the information was collected.

(3) The Directors of security and intelligence agencies may, in the notification referred to in paragraph 1 of this Article, suggest to the Chief State Attorney to postpone further actions within his/her scope of duty, if such actions might jeopardise the achievement of the objectives falling within the scope of activity of security and intelligence agencies, or endanger the safety of the employees and sources of security and intelligence agencies.

Strategic Electronic Reconnaissance for the Requirements of Security and intelligence Agencies

Article 57

(1) Strategic electronic reconnaissance for the requirements of SOA and VSOA shall be conducted by the Electronic Reconnaissance Centre of the General Staff of the Armed Forces. Planning of the strategic electronic reconnaissance implementation for the requirements of these agencies shall be done by the Council for the Coordination of Security and intelligence Agencies, at the proposal of the Directors of security and intelligence agencies. The Minister of Defence shall be in charge of the implementation of these plans.

(2) In the framework of the Chief Defence Inspection the Minister of Defence shall ensure the implementation of oversight of the legality of work of the Electronic Reconnaissance Centre of the General Staff of the Armed Forces, and shall submit reports on the Chief Inspection oversight to the Parliamentary Committee competent for national security matters.

V COOPERATION OF SECURITY AND INTELLIGENCE AGENCIES

Article 58

(1) Security and intelligence agencies shall cooperate in the performance of their functions.

(2) When a security and intelligence agency obtains any information falling within the scope of activity of the other security and intelligence agency, or when it possesses intelligence relevant for the work of the other security and intelligence agency it shall notify the said agency about these information.

(3) Security and intelligence agency may, upon the assessment that the information is necessary for the performance of its functions, request the other security and intelligence agency the information on persons under surveillance and the facts and documents it has at its disposal.

(4) In case of a possible conflict of jurisdiction security and intelligence agencies shall resolve it either in direct cooperation or within the framework of the Council for the Coordination of Security and intelligence Agencies, taking into account common national security objectives and work efficiency.

(5) Where it is not possible to reach the necessary degree of cooperation, or to resolve the issues referred to in paragraphs 2, 3 and 4 of this Article, the Council for the Coordination of Security and intelligence Agencies shall notify the National Security Council on the necessity of reaching the decision on coordinated work of security and intelligence agencies.

Article 59

(1) Security and intelligence agencies may, based on their international commitments, cooperate with foreign security, intelligence and other corresponding services through the exchange of information, equipment, through jointly conducted activities from their respective scope of work and through education of employees.

(2) The establishment and suspension of the cooperation with each foreign service shall be approved by the National Security Council on the basis of the recommendations of the Directors of security and intelligence agencies and the previously obtained opinion of the Council for the Coordination of Security and intelligence Agencies.

Article 60

(1) Security and intelligence agencies may communicate to the appropriate foreign services the information on the citizens of the Republic of Croatia if they have been provided with relevant data indicating that such person threatens the national security of the state to which data is delivered or values protected by international law. The information shall not be provided if that is either contrary to the interests of the Republic of Croatia or if the protection of the interests of the person concerned is of greater value.

(2) When security and intelligence agencies conduct security vetting requested by foreign services or international organisations for the person seeking employment in state authorities of foreign states or in the bodies of international organisations, it shall be conducted upon the receipt of a written consent of the person vetted.

(3) The delivered data shall be entered into records. Such data delivered to a foreign agency shall be accompanied by a notice indicating that they may only be used for the purpose they were provided for, and that the security and intelligence agency providing the data retains its right to request feedback on how the

provided information has been used.

VI ORGANISATION AND MANAGEMENT OF SECURITY AND INTELLIGENCE AGENCIES

Article 61

(1) Security and intelligence agencies may establish internal structural units for the purpose of performance of functions from their scope of activity and services for performing administrative and technical functions required by security and intelligence agencies and their structural units.

(2) Security and intelligence agencies may establish regional units, branch offices and temporary branch offices.

Article 62

(1) Internal organisation of security and intelligence agencies, the scope of activities of their structural units and branch offices, the manner in which these units and offices are managed, the approximate number of employees, the form, the content and the right to use the official identity card and badge, the right to carry and use weapons, the internal oversight, use and management of financial and other resources, establishment of disciplinary courts, and other matters of particular relevance for the work of security and intelligence agencies shall be determined by the Regulation passed by the Government, with the prior consent of the President of the Republic.

(2) Proposals for the Regulations referred to in paragraph 1 of this Article shall be set out by the Director of SOA for SOA and for VSOA the proposal shall be set out by the Minister of Defence.

(3) Regulations on internal structure, scope of work and management of structural units, as well as the approximate number of employees of security and intelligence agencies shall be classified and therefore shall not be published.

Article 63

(1) Pursuant to the Regulations referred to in Article 62 of this Act the modus operandi of security and intelligence agencies and their structural units, the necessary number of employees, accompanied by indications of their basic functions and tasks, their job requirements, their powers and responsibilities, rights resulting from employment as well as other relevant work-related matters not defined by this Act or the Regulations referred to in Article 62 of this Act shall be determined by Ordinances on internal order of security and intelligence agencies.

(2) The Ordinance on internal order of SOA shall be adopted by the Director of SOA with prior consent of the Head of UVNS. The Ordinance on internal order of VSOA shall be adopted by the Minister of Defence, at the proposal of the Director of VSOA, with prior consent of the Head of UVNS.

(3) Ordinances on internal order of security and intelligence agencies shall be classified and therefore shall not be published.

Article 64

(1) Ordinances on security and intelligence procedures applied by security and intelligence agencies shall define in details the procedures, measures and means used in the work, and the manner of planning, programming, implementation, recording and reporting in the work from the scope of activity of security and intelligence agencies.

(2) The Ordinance on security and intelligence procedures shall be passed by the Director of SOA, with prior consent of the Head of UVNS, while other Sub-Acts which define more specifically the procedures, measures and means used in the work, and the manner of planning, programming, implementation, recording and reporting in the work from the scope of activity of SOA shall be passed by the Director of SOA. The Ordinance on security and intelligence procedures of VSOA shall be passed by the Minister of Defence at the proposal of the Director of VSOA and with prior consent of the Head of UVNS, while other Sub-Acts regulating in details the procedures, measures and means used in the work, and the manner of planning, programming, implementation, recording and reporting in the work from the scope of activity of VSOA shall be passed by the Director of VSOA.

(3) Ordinances on security and intelligence procedures shall be classified and therefore shall not be published.

Article 65

(1) The work of security and intelligence agencies shall be managed by the Directors, and when they are prevented or absent, by Deputy Directors. The work of structural units of security and intelligence agencies shall be managed by Assistant Directors and Heads of Departments.

(2) Directors of security and intelligence agencies and their Deputies are state officials within the meaning of the Act on State Officials' Rights and Obligations.

Article 66

(1) Directors of security and intelligence agencies shall be appointed to and/or relieved from their duty by the Decision co-signed by the President of the Republic and the President of the Government.

(2) The procedure for the appointment of the Directors of security and intelligence agencies shall be initiated by the President of the Republic and the President of the Government by determining the proposal of the candidate and the previously obtained opinion of the Parliamentary Committee competent for national security. The candidate for the Director of VSOA shall be proposed to the President of the Republic and the President of the Government by the Minister of Defence. The Parliamentary Committee competent for national security may interview a candidate for the position of the Director of security and intelligence agency.

(3) The Directors of security and intelligence agencies shall be appointed for a four-year term. The person may be reappointed to the position of the Director of security and intelligence agency.

(4) The Directors of security and intelligence agencies may be relieved of their duty before the expiry of the mandate: at their own request; if they become permanently incapacitated for the performance of their duties; if they do not implement the decisions of the President of the Republic and the Government which direct the work of security and intelligence agencies, or if they fail to implement their measures related to the oversight of work; due to the violation of the Constitution, laws and other rules and regulations; the exceeding or abuse of authority; the violation of classified data secrecy, and if a final judgement for criminal offence has been pronounced against them which renders them unworthy of the position.

(5) The procedure for the dismissal of Directors of security and intelligence agencies may be initiated by the President of the Republic, the President of the Government and the Parliament of the Republic of Croatia. When the procedure is initiated by the President of the Republic or the President of the Government, before the final decision is reached, the opinion of the Croatian Parliament may be requested. When the procedure is initiated by the Croatian Parliament on account of the established breaches of law in the functioning of a security and intelligence agency or its employees, the President of the Republic and the President of the Government shall pass the decision on the dismissal of the Director of security and intelligence agency.

(6) Deputy directors of security and intelligence agencies shall be appointed to, and relieved of their duty according to the procedure and on conditions stipulated by the provisions of paragraphs 1 to 5 of this Article, but in this case the procedure shall be initiated at the proposal of the Director of security and intelligence agency and in the process of the dismissal of the Deputy Director the opinion of the Director of security and intelligence agency shall be obtained.

Article 67

(1) The internal organisation, the rules of procedure and the way of giving orders for the performance of work of security and intelligence agencies and their structural units shall be organised in such a way that individual responsibility can be established at any time.

(2) Official persons of security and intelligence agencies shall carry out the orders of their superiors, unless they consider an order to be contrary to the law, in which case they should make their written remarks, and shall then carry out the repeated written order, relieved from responsibility for the possible consequences of its execution. Where an official person assesses that the execution of the order, or the repeated written order might constitute a criminal act, he/she shall not carry it out, but shall notify immediately the Chairperson of the Council for the Coordination of Security and intelligence Agencies, the Chairperson of the Parliamentary Committee competent for national security and the Head of UVNS.

(3) Official persons who have reported the order referred to in paragraph 2 of this Article shall not be, on account of the report, submitted to any proceedings which could harm the interests of the person in question.

VII STATUS, RIGHTS, DUTIES AND RESPONSIBILITIES, AND THE PROCEDURE FOR DETERMINING SALARIES OF OFFICIALS AND EMPLOYEES OF SECURITY AND INTELLIGENCE AGENCIES, THE OFFICE OF THE NATIONAL SECURITY COUNCIL, THE INFORMATION SYSTEMS SECURITY BUREAU AND THE OPERATIONAL AND TECHNICAL CENTRE FOR TELECOMMUNICATIONS SURVEILLANCE

Implementation of Regulations

Article 68

(1) In matters not regulated by this Act provisions of the Act on Civil Servants or the Act on State Officials' Rights and Obligations shall apply to officials and employees of SOA, VSOA, UVNS, ZSIS and OTC, whereas provisions of the Act on Service in the Armed Forces of the Republic of Croatia shall apply to the employees of VSOA who are in active military service.

(2) In case they are placed at disposal, officers and employees of VSOA shall be at disposal to the Government and are entitled to the rights laid down by the Act on Civil Servants, while the active servicemen shall be at disposal to the Ministry of Defence and the Armed Forces, and are entitled to the rights laid down by the Act on Service in the Armed Forces.

Admission to Service

Article 69

(1) Public announcement of vacancies in security and intelligence agencies is not mandatory.

(2) Persons admitted to work in security and intelligence agencies, in addition to common requirements stipulated by the Act on Civil Servants, shall also satisfy specific requirements for the admission and assignment to certain jobs (specific education and profession, working experience, special skills and training, special health and psychical capabilities, etc.), stipulated by the Ordinances on internal order of security and intelligence agencies.

(3) Persons admitted to work in security and intelligence agencies shall also comply with security requirements, which is established by security vetting procedure. Security vetting shall be conducted with the approval of the person being admitted to service in security and intelligence agency and it shall cover the vetted persons' spouses and co-habitants. If the person being admitted to service does not give his/her consent for the security vetting procedure, the employment contract shall not be concluded with him/her.

(4) Persons may not be admitted to service in security and intelligence agencies if there are impediments to their admission to civil service.

(5) If a person was not admitted to work in security and intelligence agencies due to the non-compliance with the conditions or due to the presence of impediments to the admission, security and intelligence agencies need not explain the reasons for such denial.

Article 70

(1) Decisions on the admission to service and on the assignment to specific work-post shall be issued by the Director of security and intelligence agency.

(2) The Decision referred to in paragraph 1 of this Article shall not be forwarded to the central state administrative body competent for labour relations, except the Decision on placing an employee at disposal to the Government.

(3) Complaints against the Decisions referred to in paragraph 1 of this Article are not allowed, but administrative disputes may be initiated.

Article 71

(1) Employment of the persons admitted to security and intelligence agencies as trainees may be terminated during the period of their traineeship if, in the course of the traineeship, it is assessed that they do not display capabilities necessary for the performance of work in the security and intelligence agency.

(2) Complaints against the decisions on the termination of employment referred to in paragraph 1 of this Article are not allowed, but administrative disputes may be initiated.

(3) Persons hired to work in security and intelligence agencies as official persons, officers and employees shall first be accepted to a mandatory one-year probation period.

Salaries

Article 72

Salaries of the officials and employees of security and intelligence agencies shall be determined by the Government Decision in accordance with the provisions of this Act.

Article 73

(1) The salary of an official or employee of security and intelligence agencies shall be composed of the basic salary amount multiplied by the coefficient attached to specific work-posts, according to their complexity.

(2) Coefficients of the complexity of work-posts shall be determined by the Decision on salaries adopted by the Government.

(3) The basic salary amount referred to in paragraph 1 of this Article is the basic salary determined pursuant to the rules and regulations on civil servants, increased by 0,5 % for each year of working experience.

Article 74

(1) In addition to the salary determined pursuant to the provisions of Article 74 of this Act, officials and officers are entitled to bonus payments for special working conditions, risks and responsibilities.

(2) Bonus payments referred to in paragraph 1 of this Article shall be determined by the Government, as a percentage of the regular salaries received by the officials or officers.

Rights, Obligations and Responsibilities

Article 75

(1) Officers of security and intelligence agencies shall perform the work they were assigned to even in situations where their lives, health or property are at risk.

(2) Officers of security and intelligence agencies, if ordered by their superior officer, shall perform their duties even after working hours if that is necessary for the successful and timely completion of the official duty.

(3) Officers of security and intelligence agencies shall receive financial compensation or days off for their work referred to in paragraph 2 of this Article, pursuant to the Ordinance on internal order of the security and intelligence agency.

Article 76

(1) Officials and officers of security and intelligence agencies are entitled to an extended 'bonus period of pension insurance', meaning that each 12 months of actual service or employment are counted as 15, 16, 17 or 18 months of pension insurance.

(2) At the proposal of the Director of security and intelligence agency the Government shall identify work posts entitled to extended pension insurance.

Article 77

(1) Employees of security and intelligence agencies and other bodies of the security and intelligence system shall not be members of political parties, participate in the activities thereof, act on behalf of any political party within the security and intelligence agency, or perform any other public or professional function.

(2) Employees of security and intelligence agencies shall not be members of executive or managing boards of companies or corresponding bodies of other legal persons.

Article 78

Employees of security and intelligence agencies shall not, without the consent of the Council for the Coordination of Security and intelligence Agencies, make public statements or comment on the work of the agency and other bodies and persons in the field of national security, nor shall they disclose the information and documents of security and intelligence agencies to unauthorised persons.

Article 79

(1) Officials, or in other words Heads and employees of security and intelligence agencies and other bodies of the security and intelligence system, who had access to information and documents of security and intelligence agencies or other bodies of the security and intelligence system shall keep the secrecy of legally classified information and documents, regardless of the way they were disclosed to them, until they are free from keeping the secrecy thereof in a way stipulated by law.

(2) Persons referred to in paragraph 1 of this Article shall not misappropriate documents belonging to security and intelligence agencies or other bodies of the security and intelligence system.

(3) Violations of the provisions of paragraphs 1 and 2 of this Article shall be the grounds for discharge from office or termination of employment of the officials or employees referred to in paragraph 1 of this Article.

(4) Appeals against the decision on the termination of employment, referred to in paragraph 3 of this Article, are not allowed, but an administrative dispute may be initiated.

(5) Obligation to secrecy shall continue after the termination of employment of the officials or employees referred to in paragraph 1 of this Article.

(6) The Directors of security and intelligence agencies shall pass regulations on the classification of information, the procedure for handling classified information, and on special measures for the protection of classified information.

Article 80

(1) Security and intelligence agencies and other bodies of the security and intelligence system shall keep the secrecy of identity of their employees, secret collaborators, persons assisting security and intelligence agencies and other sources of information, and shall protect the manner in which the said information were obtained.

(2) In case where officers or secret collaborators of security and intelligence agencies need to testify in the proceedings conducted by judiciary bodies against individuals who were arrested as a result of the activity of the officers or secret collaborators of security and intelligence agencies, the judiciary bodies shall keep their identity secret.

Article 81

(1) Officers of security and intelligence agencies who, by the decision of the competent medical commission, were proclaimed unfit for the performance of their present jobs, either due to injury or illness which was incurred / appeared in the course of the performance of the functions stipulated by law and other regulations, shall be assigned to other functions, but shall retain the salary and other rights resulting from the employment, and if they cannot be assigned to other functions shall retain the salary and other rights resulting from the employment until they receive final decision on retirement, for the period of maximum 3 years after the decision of permanent incapacity was passed.

(2) Officers who, in the performance of their functions, or due to the performance thereof, lose their lives shall be buried in the place selected by their family, at the expense of the state budget.

(3) In cases referred to in paragraph 2 of this Article, the family of the officer shall receive single financial assistance in the amount of the last net salary received by the officer, multiplied by 12.

Article 82

(1) Person who is injured or contracts a disease while providing assistance to the officers of security and intelligence agencies in performing their duty, if not insured on other basis, is entitled to the same medical insurance rights during the treatment, as if he/she were employed in the security and intelligence agency, whereas in case of disability resulting from an injury or disease contracted while providing assistance to the officer, that person is entitled to the pension rights at the expense of the state budget.

(2) The family that loses one of its members while he/she has been providing assistance to the officers of security and intelligence agencies is entitled to the rights referred to in Article 81, paragraphs 2 and 3 of this Act.

Article 83

The Directors of security and intelligence agencies shall appoint the commission which will establish circumstances under which the officers or the person assisting the officers of security and intelligence agencies in the performance of their tasks lost their lives or contracted a disease.

Article 84

(1) If criminal proceedings have been initiated against officers of security and intelligence agencies for acts committed in the performance of the functions of security and intelligence agencies, the security and intelligence agencies shall ensure that they receive legal assistance, unless the proceedings were initiated based on the criminal report of the security and intelligence agency.

(2) Subject to the conditions referred to in paragraph 1 of this Article security and intelligence agencies shall ensure legal assistance to officers even upon the termination of their employment.

Article 85

(1) Security and intelligence agencies shall conclude life insurance contracts for their employees, or the insurance for cases of death or work-related loss of working abilities, and work-related property losses.

(2) Officers of security and intelligence agencies, depending on the complexity of their functions, are entitled to additional health insurance at the expense of the state budget.

Article 86

(1) On the basis of the Decision passed by the Minister of Defence, the Director of SOA or the Head of UVNS, the employees of VSOA, SOA and UVNS, upon the termination of service due to requirements of service, may exercise their right to old age pension, regardless of their age, when they have completed minimum 30 years of pension insurance, of which at least 15 years of pension insurance on duties or functions where the actual work performed is counted as extended period of pension insurance, pursuant to the provisions of the Act on Pension Insurance Rights of Active Servicemen, Police Officers and Civil Servants with Official Powers.

(2) Employees of security and intelligence agencies, whose employment is terminated due to the fulfilment of the conditions for retirement, are entitled to severance pay. The amount of severance pay shall be determined in the Ordinance passed by the Directors of security and intelligence agencies.

(3) Time spent at work in security and intelligence agencies which cease to exist pursuant to the provisions of this Act shall be counted as time spent at work, at adequate functions, in security and intelligence agencies.

Article 87

(1) The Republic of Croatia is accountable for all damage incurred to citizens or legal persons due to illegal, deliberate or extremely careless acts of the employees of security and intelligence agencies.

(2) The Republic of Croatia may demand from the employee of security and intelligence agency, who is found accountable for the damage referred to in paragraph 1 of this Article, to reimburse the damage compensation paid to the damaged party.

(3) Officer accountable for the damage may, for justified reasons, be partially or fully relieved of the obligation to reimburse the damage.

(4) Performance in extraordinary circumstances or in circumstances rendering impossible or difficult to avoid the damage, are considered to be justified reasons.

(5) The nature of the circumstances referred to in paragraph 2 of this Article is evaluated by the Directors of security and intelligence agencies, who shall issue written Decisions on partial or full payment acquittal.

Violation of Official Duty

Article 88

(1) For the violations of official or working duty the employees of security and intelligence agencies are accountable pursuant to the Act on Civil Servants, if otherwise not stipulated by this Act.

(2) For the violation of official, or working duty, or for disciplinary breaches or offences, the employees of VSOA are accountable pursuant to the Act on Civil Servants or the Act on Service in the Armed Forces of the Republic of Croatia, if not otherwise stipulated by this Act.

Article 89

(1) For minor breaches of official/working duty or for disciplinary breaches committed by the employees of VSOA the proceedings shall be conducted and decisions passed, at the recommendation of a superior

person, by the Directors of security and intelligence agencies, or persons designated by them.

(2) For major violations of official/working duty or for disciplinary offences, at the recommendation of the Directors of security and intelligence agencies, or persons designated by them, the proceedings shall be conducted, and the decisions reached by special disciplinary courts.

(3) Disciplinary courts of the first instance are composed of the President and five members, all appointed by the Directors of security and intelligence agencies, or by persons designated by them from among the employees of security and intelligence agencies, of whom two members and the President shall be lawyers. Disciplinary courts of the first instance shall decide in councils of three members selected by the President of the court of the first instance, separately for each individual case. The council shall always be chaired by a member appointed from among the lawyers, or by the President of the court.

(4) Disciplinary courts of the second instance are composed of the President and seven members appointed by the Directors of security and intelligence agencies, or by persons designated by them from among the employees of security and intelligence agencies, of whom the President and at least four members shall be lawyers. Disciplinary courts of the second instance shall decide in a council of three members selected by the President of the disciplinary court of the second instance, separately for each individual case. The council shall always be chaired by a member designated from among the lawyers, and it may also be chaired by the President of the court.

(5) Public shall be excluded from the proceedings against the employees of security and intelligence agencies.

Article 90

The following shall constitute minor breaches of official duty, in addition to minor breaches of official duty defined by the Act on Civil Servants and disciplinary breaches defined by the Act on Service in the Armed Forces of the Republic of Croatia:

- Unprofessional conduct by the employees of security and intelligence agencies towards the citizens or the employees of other state authorities;
- Disclosing information related to the scope of work of one structural unit of security and intelligence agency to unauthorized employees of other structural units, without prior consent of the immediate superior.

Article 91

The following constitute major violations of official duty, in addition to the violations of official duty as defined by the Act on Civil Servants and the disciplinary offences as defined by the Act on Service in the Armed Forces of the Republic of Croatia:

- Irregular spending of allocated funds, or spending for unintended purposes,
- Taking, or failure to take, any action, with a view of preventing or curbing the performance of security and intelligence agency,
- Making false statements about the security and intelligence community,
- Giving false or incomplete statements to competent oversight bodies
- Disclosing information of security and intelligence agencies to unauthorized persons, regardless of its classification level,
- Taking classified documents out of the agencies' working facilities, unless authorized to do so by the immediate superior.

Article 92

For major violations of official duty, or for disciplinary offences, the employees of security and intelligence agencies may, in addition to punishments for violations of the official duty stipulated by the Act on Civil Servants, or disciplinary punishments pursuant to the Act on Service in the Armed Forces of the Republic of Croatia, be pronounced a disciplinary punishment of termination of employment, conditionally, in the duration of 3 to 12 months.

Article 93

When an officer is removed from service, the official identification card, badge, weapons and all other means entrusted to him/her for the performance of his/her functions shall be taken away.

Relocation

Article 94

- (1) If so required for the purpose of the performance of functions, the officer may, temporarily or permanently, be relocated to another work-post in the same or different structural unit of security and intelligence agency, in the same or another work location.
- (2) Relocations lasting up to one year shall be considered temporary relocations.
- (3) Permanent relocation to another work location may be possible only with the consent of the officer concerned.
- (4) Appeals against decisions on relocation are not allowed, but an administrative dispute may be initiated.

Article 95

- (1) Any officer who is relocated to a place more than 50 km away from his place of residence is entitled to the rights pursuant to the Act on Civil Servants.
- (2) Officer relocated at his/her own request is not entitled to the rights referred to in paragraph 1 of this Article.

Article 96

- (1) Pursuant to the agreement between the Directors of security and intelligence agencies and Heads of other state authorities, an officer may, without his/her consent, be temporarily or permanently relocated to work in another state authority on an adequate work-post for which the same level of education is stipulated.
- (2) Agreement on the relocation referred to in paragraph 1 of this Article shall be concluded on the basis of staff requirements in security and intelligence agencies and other state authorities for workers with special professional skills and training, who meet the appropriate security requirements established by the security vetting procedure.
- (3) An officer relocated to another state authority may not be relocated to another work location more than 50 km away from his/her place of residence, without his/her personal consent.
- (4) Appeals against decisions on relocation are not allowed, but administrative disputes may be initiated.

Article 97

- (1) Officers of security and intelligence agencies may be sent to work abroad in the framework of cooperation with foreign security service or other corresponding service, or on the basis of an international agreement.

Article 98

Directors of security and intelligence agencies shall define in more details the rights, obligations and responsibilities of officers assigned to service to another state authority or sent for work abroad.

Termination of Service

Article 99

- (1) In addition to the cases of termination of service stipulated by the Act on Civil Servants, service of the officers of SOA shall be terminated if it is established that, by negligent performance of their functions or by violation of rules and regulations regulating the work of SOA, they have obstructed the performance of functions from the scope of activities of SOA.
- (2) In addition to the cases of termination of service defined by the Act on Civil Servants and the Act on Service in the Armed Forces of the Republic of Croatia, service of the officers of VSOA shall be terminated if it is established that by negligent performance of their functions or by violation of rules and regulations regulating the work of VSOA they have obstructed the performance of functions from the scope of activities of VSOA.
- (3) Obstructing the performance of functions referred to in paragraphs 1 and 2 of this Article includes overstepping authority or failure to exercise it, as a result of which damage was incurred to natural or legal persons, security and intelligence agencies, state authorities or the Republic of Croatia.
- (4) Decision on the termination of service in cases referred to in paragraphs 1 and 2 of this Article shall be passed by the Directors at the proposal of competent officers who have established the facts referred to in paragraph 3 of this Article.

(5) Appeals against Decisions referred to in paragraph 3 of this Article are not allowed, but administrative disputes may be initiated.

(6) When a decision on the termination of service in the case referred to in paragraph 2 of this Article is passed by the Director of VSOA for officers who are also active servicemen, their active military status and other rights related to the employment outside VSOA shall be decided by the Ministry of Defence or by the Armed Forces.

Article 100

In addition to the cases where service of officers of SOA is terminated *ex lege*, as laid down by the Act on Civil Servants, and in addition to the cases where service is terminated to officers of VSOA *ex lege*, as laid down by the Act on Civil Servants or the Act on Service in the Armed Forces of the Republic of Croatia, the service is also terminated *ex lege*:

- when the competent body establishes that he/she has met the conditions for the retirement on account of general or professional incapacity – on the day the decision becomes final,
- when it is established that the employee has given false information at the time of admission to service - on the day when the deception is revealed,
- when an officer is convicted for a criminal offence prosecuted *ex officio*, except for the offences referred to in Title XX of the Criminal Act of the Republic of Croatia, related to transport security - on the day when the verdict becomes final,
- if an officer refuses legal relocation – on the day when he/she is supposed to report to duty,
- when it is discovered that the officer has acted contrary to the provision of Articles 77 and 78 of this Act – on the day the violation is revealed,
- when it is learnt that he/she has acted contrary to the provisions of Article 79, paragraphs 1 and 2 of this Act – on the day this violation is revealed.

Article 101

If the competent health commissions of security and intelligence agencies or UVNS pronounce the employee incapable to continue working, then the competent expert referred to in Article 113, paragraph 1 of the Pension Insurance Act shall establish that such employee is professionally or generally incapable for work in accordance with the provisions of the Pension Insurance Act.

Article 102

(1) On the basis of the Decision of the Director of security and intelligence agency or the Head of UVNS, the employees of security and intelligence agencies who have completed 20 years of insurance of which they have at least spent 10 years at duties or functions where active work is counted as prolonged period of pension insurance, and who by appropriate procedure have been found incapable of further professional growth, service may be terminated due to professional incapacity for work, with entitlement to disability pension.

(2) Appeals against decisions referred to in paragraph 2 of this Article are not allowed, but administrative disputes may be initiated.

VIII OVERSIGHT OVER THE WORK OF SECURITY AND INTELLIGENCE AGENCIES

Article 103

The oversight over security and intelligence agencies shall be conducted by:

- the Croatian Parliament
- the Office of the National Security Council
- the Council for the Civilian Oversight of Security and intelligence Agencies

Article 104

(1) The oversight of security and intelligence agencies by the Croatian Parliament shall be conducted directly and through the Parliamentary Committee competent for national security, and the Council for the Civilian Oversight of Security and intelligence Agencies

(2) In the effectuation of the oversight referred to in paragraph 1 of this Article the Croatian Parliament may request:

- from a security and intelligence agency reports on actions and measures implemented by the security and intelligence agency,
 - from the President of the Supreme Court of the Republic of Croatia reports on the measures of secret information gathering or on the implementation of secret information gathering applied against certain persons,
 - from security and intelligence agencies reports on the implementation of measures of secret information gathering or on the implementation of measures of secret information gathering applied against certain persons,
 - the report on whether security and intelligence agencies have collected information regarding any Member of Parliament or any person from their household,
- (3) In the effectuation of the oversight referred to in paragraph 1 of this Article the Croatian Parliament, or the Parliamentary Committee competent for national security may request that UVNS submits reports and information, and/or to perform professional oversight of security and intelligence agencies.
- (4) Parliamentary Committee competent for national security may also perform direct oversight of the work of security and intelligence agencies.
- (5) When direct oversight is performed by the Parliamentary Committee competent for national security provisions of this Act regulating the professional oversight activity of UVNS shall apply.

Article 105

- (1) In addition to matters referred to in Article 104, paragraph 2 of this Act, to be discussed by the Committee of the Croatian Parliament competent for national security, the Committee is also authorized to summon the Directors and officers of security and intelligence agencies to hearings regarding the illegality of the application of certain measures and actions by the agencies, to discuss the legality of financial and material management of security and intelligence agencies, to review the Ombudsman's reports on the protection of constitutional and legal rights of citizens in the procedures undertaken by security and intelligence agencies, and to look into the work of security and intelligence agencies with respect to the foreign policy of the Republic of Croatia.
- (2) When the Croatian Parliament or the Croatian Parliamentary Committee competent for national security request reports, documentation or necessary data from security and intelligence agencies, the Council for the Coordination of Security and intelligence Agencies or from the President of the Supreme Court of the Republic of Croatia in the case referred to in Article 104, paragraph 2, item 3 of this Act, they shall immediately notify UVNS thereof, and invite the Head of UVNS and the Director of the competent security and intelligence agency to be present at the meeting where matters from the scope of activity of security and intelligence agency shall be discussed.
- (3) Information disclosed to the Croatian Parliament or the Parliamentary Committee competent for national security shall not include information on the persons with whom the security and intelligence agency has collaborated in the performance of its functions, or information obtained from foreign intelligence services, unless the consent of the said service or the decision of the National Security Council is obtained.
- (4) The work of the Parliamentary Committee competent for national security is chaired by the Member of Parliament from the benches of the largest opposition party.

Professional Oversight of the Work of Security and intelligence Agencies

Article 106

Professional oversight of the work of security and intelligence agencies and of OTC shall be performed by UVNS.

Article 107

- (1) Within the framework of professional oversight functions UVNS shall:
- monitor and control the legality of work,
 - monitor and control the achievement of prescribed goals and scope of work
 - monitor and control the effectiveness and usefulness of work,
 - control the application of measures of secret information gathering that restrict constitutional rights and basic human freedoms,
 - control the use of financial resources,
 - supervise the coordination and cooperation between security and intelligence agencies and the

corresponding foreign services.

(2) When performing the functions referred to in paragraph 1 of this Article UVNS may have access to the reports and other documents of security and intelligence agencies and OTC, may conduct interviews with the Directors and employees of security and intelligence agencies and OTC if that is necessary in order to establish the facts crucial for the evaluation of the legality of work.

Article 108

(1) Security and intelligence agencies shall permit the officers of UVNS, at their request, to have access to data concerning the identity of agency's sources only if that is necessary for the fulfilment of the final oversight goals in the specific case.

(2) In case of an explicit disagreement with the request referred to in paragraph 1 of this Article the Directors of security and intelligence agencies shall request the Decision on the specific case to be made by the National Security Council.

Article 109

(1) When, in the performance of the functions referred to in Article 107, paragraph 1 of this Act, UVNS establishes that actions of security and intelligence agencies have been, or are, violating the Constitution and laws of the Republic of Croatia, the Head of UVNS shall undertake measures for immediate removal of the detected irregularities, and shall inform the President of the Republic, the President of the Government and the President of the Croatian Parliament thereof if the inspection was performed at the request of the Croatian Parliament, or the Parliamentary Committee competent for national security.

(2) Measures referred to in paragraph 1 of this Article undertaken by UVNS shall be regulated in detail by the Regulation referred to in Article 11 of this Act.

Civilian Oversight of the Work of Security and intelligence Agencies

Article 110

(1) For the purpose of ensuring the civilian oversight of the work of security and intelligence agencies the Council for the Civilian Oversight of Security and intelligence Agencies shall be established (hereinafter: the Council).

(2) The Council shall be composed of the Chairperson and six members, all appointed by the Croatian Parliament.

(3) Appointed members of the Council shall have university degree, and shall include at least one member who has a degree in law, one member with a degree in political sciences and the one with a degree in electro-technical sciences.

(4) The Chairperson and the members of the Council shall be appointed for a period of four years, and may be reappointed after the expiry of the first term.

(5) For the legality of their work, the Chairperson and the members of the Council shall be responsible to the Croatian Parliament, while the Parliamentary Committee competent for national security shall be competent for the oversight of the legality of their work.

(6) Matters relevant for the work of the Council not regulated by this Act, and the performance of the administrative work for the Council shall be regulated by the Act of the Croatian Parliament at the proposal of the Parliamentary Committee competent for national security.

Article 111

(1) The Council shall perform the following functions:

- monitoring the legality of work of security and intelligence agencies,
- monitoring and controlling the implementation of the measures of secret information gathering that restrict the basic human rights and freedoms laid down by the Constitution,
- delivering, in the form of information, the obtained information and data referred to in previous items, to the National Security Council, the President of the Parliament, the President of the Parliamentary Committee competent for national security, and to the Directors of security and intelligence agencies; and
- providing information about the procedure for submitting the request referred to in Article 112 of this Act.

(2) While performing the works referred to in paragraph 1 of this Article the Council may have access to reports and other documents of security and intelligence agencies, may interview Directors and officers of security and intelligence agencies when it is necessary in order to determine facts crucial for the assessment

of the legality of work of security and intelligence agencies.

Article 112

Council shall perform the functions referred to in Article 111 of this Act pursuant to the Programme adopted by the National Security Committee, based on the requests submitted by citizens, state authorities and legal persons, regarding the observed unlawful actions or irregularities in the work of security and intelligence agencies, especially in cases of violations of basic freedoms and human rights guaranteed by the Constitution.

Article 113

- (1) The information regarding the conducted oversight inspection shall be reported to the person who had submitted that request.
- (2) In its reply to the submitted request the Council shall refer only to the remarks listed in the request.
- (3) Where, in the conducted oversight, it is established that there have been some unlawful acts, the Chairperson of the Council shall notify the President of the Republic of Croatia, the President of the Parliament, the President of the Government and Chief State Attorney about the results of the oversight.
- (4) At the request of the President of the Parliament, and at least once every six months, the Chairperson of the Council shall submit reports on the work of the Council.

Article 114

- (1) The Chairperson and members of the Council shall keep the secrecy of information they have learned while performing the functions in the Council.
- (2) The obligation referred to in paragraph 1 of this Article shall continue after the termination of the function in the Council.

IX RESOURCES FOR THE WORK OF SECURITY AND INTELLIGENCE AGENCIES, THE OFFICE OF THE NATIONAL SECURITY COUNCIL, INFORMATION SYSTEMS SECURITY BUREAU AND OPERATIONAL AND TECHNICAL CENTRE FOR TELECOMMUNICATIONS SURVEILLANCE

Article 115

- (1) The resources for the work of security and intelligence agencies, UVNS, ZSIS and OTC shall be secured from the state budget.
- (2) The resources for the work of security and intelligence agencies, UVNS, ZSIS and OTC shall also include special resources for working premises, technical equipment, special purposes in the performance of intelligence and counterintelligence functions, education, instruction and training of the employees of security and intelligence agencies, and measures of concealment.

Article 116

Provisions regulating functioning of state authorities shall appropriately apply to the financial and material dealings of security and intelligence agencies, UVNS, ZSIS and OTC. Information regarding the financial and material dealings shall be kept secret.

X TRANSITIONAL AND FINAL PROVISIONS

Article 117

- (1) The Government shall pass the Regulations on internal organisation of security and intelligence agencies, UVNS, ZSIS and OTC, and other rules and regulations stipulated by this Act, within 30 days from the date this Act enters into force.
- (2) Ordinances on internal order and Ordinances on the procedures for the functioning of security and intelligence agencies, Ordinances on the internal structure and other Ordinances of UVNS shall be passed within 60 day following the date when this Act enters into force.

Article 118

The Director of SOA, the Director of VSOA and the Head of UVNS shall be appointed within 15 days following the date when this Act enters into force.

Article 119

- (1) The Director of ZSIS shall be appointed within 30 days following the date when this Act enters into force
- (2) Ordinance on the internal structure of ZSIS and other Ordinances regulating its work shall be passed within 60 days following the date when this Act enters into force.

Article 120

- (1) On the date when this Act enters into force SOA, VSOA and ZSIS shall begin to function, while the Intelligence Agency (OA), the Counterintelligence Agency (POA) and the Military Security Agency (VSA) and the Institute for Information Security and Crypto-technology shall cease to operate.
- (2) The internal structural units of OA and POA shall continue their work as the internal structural units of SOA, until the date when the Ordinance on the internal structure of SOA enters into force.
- (3) On the date when this Act enters into force the employees of the Intelligence agency (OA) and the Counterintelligence Agency (POA) shall become employees of SOA, while the employees of the Military Security Agency (VSA) become employees of VSOA and, until the adoption of new Ordinance on the internal order of SOA or VSOA respectively, they shall continue performing the tasks they were performing on the day of entry into force of this Act.

Article 121

- (1) The employees of the Intelligence agency (OA), the Counterintelligence Agency (POA) and the Military Security Agency (VSA) shall continue to work at the work posts they were filling on the day when this Act enters into force, and shall keep the salary and bonuses determined by the currently applicable Decisions, until new Decisions are passed on their assignment to work posts established by the Ordinances on internal order of SOA and VSOA.
- (2) Employees of security and intelligence agencies may be assigned to work posts requiring education level one degree higher than the one they have obtained, on condition that within four years following the assignment they obtain the required level of education.
- (3) The employees of SOA who refuse the assignment, and the employees of VSOA who refuse the assignment or are not offered one, shall be placed at disposal to the Government, safe for the active servicemen - employees of VSOA, who shall be placed at the disposal of the Ministry of Defence and the Armed Forces.

Article 122

- (1) On the date when this Act enters into force the facilities, equipment, devices, archives and documentation, and other resources of the Intelligence Agency and the Counterintelligence Agency shall be taken over by SOA, of the Military Security Agency shall be taken over by VSOA, and of the Institute for Information Security and Crypto-Technology shall be taken over by ZSIS, unless the President of the Republic and the Government decide otherwise by consensus.
- (2) Until the date when the Ordinance on the intelligence and security procedures, and other implemented rules and regulations of SOA and VSOA enter into force, provisions of the currently valid Acts regulating the intelligence or security procedures for the functioning of the Intelligence Agency, the Counterintelligence Agency and the Military Security Agency shall be valid, unless they become contrary to the provisions of this Act.

Article 123

The OTC shall be established within the period of maximum one year from the date when this Act enters into force. Until the establishment of OTC the functions from the scope of competence of OTC shall be performed by the Operational and Technical Centre for the Interception of Telecommunications of Security and intelligence Agency.

Article 124

Provisions of paragraph 4 of this Article shall be applied on the date of the constitution of the new assembly of the Croatian Parliament, following the next parliamentary elections.

Article 125

(1) On the date when this Act enters into force, the Act on Security Services of the Republic of Croatia (Official Gazette, No. 32/02 and 38/02) shall cease to be valid.

(2) On the date when this Act enters into force the Regulation of the Government of the Republic of Croatia on the establishment of the Institute for information security and crypto-protective technology shall cease to be valid.

(3) On the day of entry into force of the Regulation referred to in Article 20, paragraph 1 of this Act, the currently valid Regulation on the obligations in the field of national security of the Republic of Croatia for legal and natural persons in telecommunications shall cease to be valid.

Article 126

This Act shall enter into force 30 days following its publication in the Official Gazette.

Class: 215-01/06-01/04

Zagreb, 30 June 2006

CROATIAN PARLIAMENT
THE PRESIDENT OF THE PARLIAMENT

Vladimir Šeks, m.p.