Bogoljub Milosavljevic

PROPOSED SOLUTIONS FOR IMPROVING THE LEGAL FRAMEWORK ON THE SERBIAN SECURITY AND INTELLIGENCE SYSTEM
PROPOSED SOLUTIONS FOR IMPROVING THE LEGAL FRAMEWORK ON THE SERBIAN SECURITY AND INTELLIGENCE SYSTEM

Publisher
Belgrade Centre for Security Policy
6 Djure Jaksica Street, Belgrade
Telephone: +381 11 3287 226
E-mail: office@bezbednost.org
Web: www.bezbednost.org

Author
Prof. Bogoljub Milosavljevic PhD

Translation from Serbian
Vera Gojkovic

Design and layout
Marko Marinkovic

ISBN
978-86-6237-142-3

Belgrade, 2017

Publication of this study was kindly supported by The Embassy of the Kingdom of the Netherlands in Belgrade, in the framework of the project “LEGASI - Towards Legislative Reform of Security Intelligence System”. The opinions expressed in the publication are solely those of the author and do not necessarily reflect the positions of the Kingdom of the Netherlands.
1. INTRODUCTORY NOTES

This document has been developed by the Belgrade Centre for Security Policy as a type of “legislative agenda” made within the LEGASI Project – Towards Legislative Reform of Security and Intelligence System. It is made up of proposed legal solutions, which, if incorporated in relevant laws, could improve the existing legal framework on the Serbian security and intelligence system. All proposals directly rely on the (1) March 2016 Analysis of the Legal Organization of the Security and Intelligence System of the Republic of Serbia, and (2) Model Law on Security Services of the Republic of Serbia, whose final version was developed in September 2016, as well as on other ideas, suggestions and proposals obtained during expert consultations with representatives of some state authorities, academic community, media and NGOs in different stages of project realization.

The proposals are systematized according to significant groups of issues, or legal instruments. Each group of proposals contains a brief description of the observed issue and its possible solution, which is followed by legal provisions formulated as amendments through which the relevant solution would be implemented after its inclusion in the laws. In order to make things easier, the proposals are grouped around the three existing laws (1) Law on the Bases Regulating Security Services of the Republic of Serbia (hereinafter referred to as: the ZOUSB), (2) Law on the Security Information Agency (hereinafter referred to as: the Law on the BIA) and (3) Law on the Military Security Agency and Military Intelligence Agency (hereinafter referred to as: the Law on the VBA and VOA).  

As a whole, the proposals are meant to serve as a less successful alternative to the certainly more appropriate core idea - to have a unified new law on security services that would replace the three existing laws that cover the same issue, as suggested in the Model Law on Security Services of the Republic of Serbia. To that effect, the proposals provided in this document are limited to legally implementable innovations of the three existing laws and their scope is more limited than the possible improvement that would be achieved through the development of a single law on security services. This primarily refers to the reorganization of security services, whose number, according to the new Model Law, would be reduced to two from the current three, as well as to a number of other innovations contained in the Model, including a set of minor corrections that need to be made in the existing legal framework. Additionally, this approach, as partial, does not ensure the normative rationalization and harmonization of some solutions in the three laws.

---

1 Law on the Bases Regulating Security Services of the Republic of Serbia was adopted in 2007 and amended in 2012 (Official Gazette of the RS No. 116/07 and 72/12), Law on the Security Information Agency was adopted in 2002 and amended in 2009 and 2014 (Official Gazette of the RS No. 42/02, 111/09, 65/14 – CC decision and 66/14), while the Law on the Military Security Agency and the Military Intelligence Agency was adopted in 2009 and amended in 2012 and 2013 (Official Gazette of the RS No. 88/09, 55/12 – CC decision and 17/13).
2. PROPOSALS FOR THE IMPROVEMENT OF THE ZOUSB

2.1. Security and Intelligence System of the Republic of Serbia

Description of the Issue

The existing formulation of the principles of operation of security services (Article 2 of the ZOUSB) does not express their meaning in a sufficiently strong and precise manner, which paves the way to the appearance of other, primarily extralegal factors, which occasionally visibly undermine the desired level of political neutrality in the operation of security services. Even the formulation contained in Article 3 paragraph 1 of the ZOUSB, which regulates the security and intelligence system, is incomplete, because it does not show that security services represent an integral part of the national security system of the Republic of Serbia (as they are defined in the National Security Strategy of the Republic of Serbia). Provisions on cooperation among security services and exchange of information are also lacking.

Possible Solution

These shortcomings can be removed relatively easily through the introduction of additional provisions in the above mentioned articles of the ZOUSB, which would more clearly and comprehensively determine the principles of operation of security services and define them as an integral part of the national security system. Special provisions would regulate the issue of cooperation among security services and data exchange.

Proposed Amendments

Article 1

Article 2 of the ZOUSB is to be amended as follows:

„Article 2 Principles of Operation of Security Services

1. In carrying out activities within their competence, security services are autonomous and they operate on the basis and within the Constitution, laws, other regulations and general acts, national security strategy and policy, defense strategy and policy, as well as the security and intelligence policy of the Republic of Serbia.

2. The autonomy of security services in carrying out their activities means that they have operative autonomy and the right, based on their legal competences and own responsibility and without unauthorized interference and influence of other subjects, to plan and implement operations and measures in order to perform activities within their competence.

3. Security service members are required to act in accordance with the Constitution, law, other regulations and general acts, and to observe human rights and freedoms, professionalism and proportionality in the implementation of their competences.

4. Within their operation, security services are unbiased, politically and ideologically neutral, and must not undertake any activities to the prejudice of any political party or interest group."
5. The director and members of a security service must not be political party members.
6. Security service members may be organized within trade unions and may establish professional and expert associations within their security service.
7. Security services may not exert police authority, with the exception of legally defined authority.

**Article 2**

Article 3 paragraph 1 of the ZOUSB is amended as follows:

„Security services constitute a part of the security and intelligence and national security systems of the Republic of Serbia.“

**Article 3**

A new Article 3a is inserted after Article 3 of the ZOUSB, and it reads as follows:

„Article 3a Cooperation among Security Services and Information Exchange

1. Security services cooperate with each other and exchange information, in accordance with the relevant government regulation.
2. Security services cooperate and exchange information with competent authorities, organizations and institutions of the Republic of Serbia, as well as foreign security services and international organizations, in accordance with the Constitution, law, other regulations and general acts, the defined security and intelligence policy of the Republic of Serbia and ratified international treaties.
3. On the basis of a written decision of a security service director, relevant foreign security services and international organizations may be sent information about citizens of the Republic of Serbia and persons with the temporary place of residence in the Republic of Serbia under the conditions referred to in paragraph 2 of this Article, but only after the provision of irrefutable evidence that such a person is a threat to security or values protected by international law.
4. Security services will not send information referred to in paragraph 3 of this Article if this would undermine the interests of the Republic of Serbia or unproportionally undermine the interests of the person to whom such information refers. The security service director will determine if there exist obstacles to the sending of information upon obtaining the opinion of the Council.
5. The disclosed data are accompanied by a note saying that the data may be used only for the requested purpose, as well as that the security service which has sent the data reserves the right to be informed about the way in which the data are used. The circle of all possible data users is also defined in the note.
6. Security services keep the records pertaining to the submitted data referred to in paragraph 3 of this Article.“

**2.2. Directing and Harmonizing the Operation of Security Services**

**Description of the Issue**

According to the ZOUSB, the National Security Council is a state authority of the Republic of Serbia which looks after the national security and which is in charge of directing and harmonizing the work of security services, on the one hand, and of controlling it, on the other, while the operative harmonization of the work of security services is within the competence of the Coordination Bureau for Security Services, made up of the secretary of the National Security Council and directors of security services. However, not all aspects
of the Council's competences and composition have been regulated appropriately (incomplete description of competences, the minister of foreign affairs and the National Assembly speaker are not among its members), nor has the obligation of this authority to report to the National Assembly on its operation been regulated. The appointment and dismissal of the Council secretary, who also manages the work of the Bureau, has been left to the president of the Republic under a blanket norm, without the imposition of an obligation to consult other authorities about it.

Possible Solution

The competences of the National Security Council need to be specified (Article 5 of the ZOUSB), its composition expanded (Article 6) and the obligation to consult the National Assembly and the government about the person who is being appointed Council secretary needs to be imposed (Article 7 paragraph 3 of the same Law).

Proposed Amendments

Article 4

Article 5 of the ZOUSB is amended as follows:

„Article 5 Competence of the Council

1. The National Security Council of the Republic of Serbia (hereinafter referred to as: the Council) performs tasks of importance for directing and harmonizing the work and control of the operation of security services.

2. In the performance of activities referred to in paragraph 1 of this Article, the Council:
   1) Reviews the proposed national security strategy, proposed defense strategy and doctrine, and proposals of other strategies and laws of importance for the security of the Republic of Serbia;
   2) Reviews parts of the proposed foreign policy strategy that are important for the security of the Republic of Serbia;
   3) Reviews security and intelligence assessments and develops guidelines and conclusions on the ways and priorities of protection and realization of national interests of security and intelligence activities;
   4) Monitors the implementation of adopted guidelines and conclusions;
   5) Reviews the cooperation between security services and foreign security services and provides guidelines for its implementation;
   6) Reviews and provides its opinion on proposed annual and medium-term security service action plans;
   7) Reviews regular and special activity reports of security services;
   8) Gives its opinion on the proposed security service budgets and monitors the expenditure of funds;
   9) Reviews the operation of security services and the Bureau for the Coordination of Operation of Security Services, and makes relevant conclusions thereon;
   10) Provides guidelines for the harmonization of operation of security services and monitors their implementation;
   11) Gives its opinion on proposals for the appointment and dismissal of security service directors;
   12) Gives its opinion on proposals for the appointment and dismissal of the inspector-general of security services and the Technical Operational Center;
13) Reviews activities within the scope of work of authorities belonging to the state administration, territorial autonomy and local governance, which are of importance for the realization of national security interests;
14) Looks after the harmonized implementation of regulations and standards on personal data protection and other regulations protecting human rights that may be violated through the exchange of information or other operative activities of the security services;
15) Also reviews other issues in accordance with the law.

3. The Council files its reports to the National Assembly once a year, and if necessary, also files special reports on its operation and informs the public about its work in accordance with the law."

**Article 5**

In Article 6 of the ZOUSB, after the first bullet point, a new bullet point is added, which reads „National Assembly speaker;“ after the fourth bullet point, a new bullet point is added, which reads „the minister of foreign affairs“ and after the seventh bullet point, a new bullet point is added, which reads „police director.“

**Article 6**

Article 7 paragraph 3 of the ZOUSB is amended as follows:

„The Council secretary is appointed and dismissed by the president of the Republic, after obtaining the opinion of the government and the National Assembly committee responsible for controlling security services.”

### 2.3. Supervision of the Operation of Security Services

**Description of the Issue**

Under the Law on the VBA and VOA, the inspector-general is one of the authorities responsible for supervising these security services (Articles 54 through 56). The inspector-general exists parallel with internal control bodies, and is appointed by the government to a five-year term of office. As opposed to this, in the case of the BIA there is just internal control, which, like other similar control mechanisms (established within some other state administration bodies), operates as an internal control mechanism, with the obligation to report about its control findings to the top manager, or in this case the BIA director. Through his/her position and role, the inspector-general ensures better control, including the possibility to inform the government and the competent National Assembly committee about possible omissions in the work of security services.

**Possible Solution**

Starting from the assessment that an inspectorate-general for all three security services would represent a more appropriate solution than separate inspectors-general for the BIA and the military security services, we have herein proposed an amendment to the ZOUSB that would regulate the issue. This solution would require that the existing provisions on the inspector-general be deleted from the Law on the VBA and VOA.
Proposed Amendments

**Article 7**

After Article 20 of the ZOUSB, Articles 20a and 20b are added, which read as follows:

„Article 20a Inspectorate-General of the Security Services

1. The Inspectorate-General of Security Services is established as a separate government agency for the purpose of supervising the operation of security services and the technical Operative Centre, in accordance with this Law.

2. The work of the Inspectorate-General is managed by the inspector-general, whom the government appoints to a five-year term of office upon obtaining the opinion of the Council and the National Assembly committee responsible for controlling security services.

3. The competences of the Inspectorate-General may be discharged by the inspector-general and inspectors, each of whom will be supervising one of the security services and the Technical Operational Center (alternatively: inspectors are appointed for individual areas of operation, e.g. for the implementation of special procedures and measures for the covert collection of data, for the political and interest neutrality of operation of security services, etc.).

4. Persons with at least nine years of professional experience, who are not political party members, who do not hold other public offices and who fulfill other legally defined conditions as well as the conditions pertaining to the absence of security threats may be appointed inspector-general and inspectors.

5. The inspector-general and inspectors have the status of civil servants discharging an office, defined under a government document in accordance with the law.

**Article 20b Activities of the Inspectorate-General and Competences of Inspectors**

1. The Inspectorate-General:
   1) as impartiality in the work of security services and their members;
   2) Oversees the lawfulness of operation of security services, particularly the lawfulness of implementation of special procedures and covert data collection measures;
   3) Determines facts on the observed violations of law and irregularities in the operation of security services and their members;
   4) Oversees the lawfulness and regularity of operation of the Technical Operational Center;
   5) Files reports on the results of oversight to the government, Council and competent National Assembly committee responsible for controlling security services.

2. Oversees the implementation of the principles of political, ideological and interest neutrality, as well within the scope of their work, the inspector-general and inspectors are authorized to enter the premises of security services and the Technical Operational Center, to inspect documents, to get the necessary data and information on the work of security services and the Technical Operational Center and to interview the manager and members of security services, or the manager and employees of the Technical Operational Center, in order to determine facts of importance for performing tasks referred to in paragraph 1 of this Article.

3. The inspector-general and inspectors may not get the data referred to in Article 19 paragraph 2 of this Law.

4. The inspector-general, inspectors and other Inspectorate-General employees are required to protect and maintain the confidentiality of information and data they learn of in the scope of their work even after they stop working at the Inspectorate-General."
2.4. Technical Operational Center

Description of the Issue

The ZOUSB regulates the parliamentary oversight of the implementation of special procedures and measures for the covert collection of data by security services, while the measures themselves and the approval procedure are regulated by the Laws on the BIA, and on the VBA and VOA. In addition to this, the Criminal Procedure Code regulates special investigative measures, some of which are the same, according to their content, as the above mentioned special procedures and measures, and the court may authorize the police, BIA, VBA and some other state authorities to implement these measures or means. The existing legal solutions practically make it possible for each of the authorized subjects to implement special procedures and measures independently, if they have the necessary technical capacity for this purpose at their disposal. These solutions create practical problems which, inter alia, increase the risk from the insufficiently controlled encroachment on citizens’ privacy.

Possible Solution

As a possible solution to this issue, several players, particularly the ombudsman and commissioner for information of public importance and protection of personal data, have proposed the establishment of a separate institution, based on the model of some other countries, which would technically implement the surveillance of electronic communications, telecommunication services and IT systems, without having an insight into the collected data, and acting for the needs of security services, police and other authorized authorities. In terms of law, the most effective solution would be to have a separate law adopted on such an institution, or to have it regulated in a unified law on security services. The next attainable solution offered herein would be to amend the ZOUSB by adding a new chapter that would regulate the establishment and functioning of this institution (Technical Operational Center).

Proposed Amendments

Article 8

In the ZOUSB, after Article 21, a new chapter is added „IVa TECHNICAL OPERATIONAL CENTER“ as well as Articles 21a, 21b, 21g and 21d, which read as follows:

„Article 21a Establishment and Activities of the Technical Operational Center

5. For the purpose of performing activities referred to in this Law, the government will establish the Technical Operational Center within one year after the date when this Law takes effect, and secure the necessary conditions for the beginning of its operation.

6. The Technical Operational Center, in accordance with this Law, the law that regulates criminal procedure, laws on security services and laws that regulate electronic communications and telecommunications:

1) Provides technical services for the needs of security services, police and other state authorities within their legal competences for the implementation of special procedures and measures or special investigative measures through which the covert surveillance of electronic communications, telecommunication services and IT systems is conducted;
2) Ensures operative and technical coordination between security services, police and other state authorities in the implementation of special procedures and measures, or investigative means referred to in item 1 of this paragraph;
3) Ensures the indelible registration of access to electronic communications, telecommunications and IT systems, with all data necessary for the subsequent control of lawfulness and regularity of access;
4) Keeps a register of orders and ordinances and other data on the implementation of special procedures and measures or special investigative measures used for the covert surveillance of electronic communications, telecommunication services and IT systems.

7. The way in which activities referred to in paragraph 2 of this Article are performed is more closely regulated by the government, upon obtaining the opinion of the Council and National Assembly committee responsible for controlling security services.

Article 21b. Operation Management

1) The director manages and is responsible for the operation of the Technical Operational Center.
2) The director is appointed by the government to a five-year term of office, at the proposal of the prime minister, after obtaining the opinion of the Council and National Assembly committee responsible for controlling security services.
3) The director may not discharge any other public office.
4) The director has a deputy who is appointed in the same way and under the same conditions as the director.
5) The director files the annual report on the operation of Technical Operational Center to the government, the Council and National Assembly committee responsible for controlling security services, and, at their request or according to his own assessment, other reports as well.

Article 21v Special Conditions for the Director and Employees

8. The director, deputy director and employees at the Technical Operational Center must have certificates for accessing secret data in accordance with the law, as well as IDs, the appearance of which is determined by the government.
9. The director, deputy director and employees at the Technical Operational Center may not be political party members.

Article 21g Special Responsibilities of the Director and Employees

1) The director, deputy director and employees at the Technical Operational Center may not have an insight into the contents of communications and other data on communications obtained through the implementation of covert interception of communications, telecommunication services and IT systems.
2) The director, deputy director and employees at the Technical Operational Center are required to refuse to act at the request of security services, police and other state authorities to implement the covert interception of communications, telecommunication services and IT systems if the request has not been issued in accordance with the law and to notify the prime minister thereof without delay.
3) The duty to refuse the request and the duty of notification without delay referred to in paragraph 2 of this Article also exist in the case where the request is received from any other incompetent state authority, official or another subject.
4) The director, deputy director and employees at the Technical Operational Center are required to keep secret anything they know about the implementation of special procedures and measures, or special investigative measures.
5) The violation of paragraphs 1 through 4 of this Article represents the reason for the dismissal of the director and deputy director of the Technical Operational Center, or a more serious violation of work duty for which the measure of termination of employment is imposed on the employee.

3. PROPOSALS FOR THE IMPROVEMENT OF THE LAW ON THE BIA

3.0. Preliminary Remarks

In view of the fact that, with the exception of innovated provisions on special procedures and measures for the covert collection of data from 2014, the Law on the BIA regulates in a rather modest manner the competence and activities, organizations, methods of work, control of operation as well as the position of the security service members, it is clear that the best effects would be achieved through the drafting and adoption of a new law on this security service, or a single law on the security services, as proposed in the Model Law on the Security Services of the Republic of Serbia. Starting from this premise, only the most important proposals for improving the existing law are elaborated hereinafter.

3.1. Competences and Operation of the BIA

Description of the Issue

The BIA competences and operations are regulated by Article 2 of the Law on the BIA through the following formulation: „The Agency carries out tasks relating to: the security of the Republic of Serbia; the discovery and prevention of activities which threaten to undermine or disturb the constitutional order of the Republic of Serbia; the acquisition, processing and analysis of security and intelligence information relevant to the security of the Republic of Serbia; and informing the competent state authorities about the data as well as other activities determined by the law.” Additionally, Article 16 paragraphs 1 and 2 of this Law say that if required because of special security reasons of the Republic of Serbia, the BIA can take over and directly carry out certain activities that are within the competence of the Ministry responsible for internal affairs, on the basis of a decision reached in agreement between the BIA director and the minister responsible for internal affairs. Thus defined, BIA competences and operations are insufficiently specified and demarcated from the competences and operations of other security services and security authorities. In addition to this, the Law on the BIA does not impose the obligation on this security service to establish cooperation with the competent military security service if measures are implemented against persons working at the Ministry of Defense and Serbian Army.

Possible Solution

The existing provisions of Article 2 of the Law on the BIA may be replaced in the same law by more complete and more precise provisions on the competences and operations of the BIA, as well as on its cooperation with the competent military security service.
Proposed Amendments

Article 1

Article 2 of the Law on the BIA is amended as follows:

Article 2

1. The BIA is in charge of intelligence and security activities of importance for the protection of security of the Republic of Serbia, and of preventing a forcible change of its constitutional order.
2. While performing intelligence activities, the BIA collects, registers, keeps, processes, analyzes and sends to competent state authorities data and information about security threats against the Republic of Serbia and its citizens.
3. While performing security activities, the BIA in the territory of the Republic of Serbia detects, foresees, prevents, removes and documents security threats against the Republic of Serbia and its citizens that result from the activities of organizations and persons involved in organized crime activities and criminal offenses with an international dimension, terrorism and the most serious types of criminal activities against humanity and international law, and against the constitutional order and security of the Republic of Serbia.
4. Whenever required by special security reasons of the Republic of Serbia, the BIA may take over and directly perform certain activities within the competence of the ministry responsible for internal affairs on the basis of a decision reached in agreement between the BIA director and minister responsible for internal affairs.
5. While performing activities referred to in paragraphs 3 and 4 of this Article, the BIA may implement measures against persons serving at the Ministry of Defense and Serbian Army only with a written notification of the head of the Military Security Agency and in cooperation with the VBA.

Article 2

After Article 2 of the Law on the BIA, Articles 2a through 2d are added and they read as follows:

Article 2a

6. The BIA performs the security protection of institutions, persons, objects and areas of special security importance, in accordance with a government regulation.
7. While performing security protection activities, the BIA within its scope of work makes security assessments of possible threats and uses them to implement the measures of protection from eavesdropping and protection of confidential communications, performs security checks of persons who have access to protected institutions, persons, facilities and spaces, and participates in the planning, implementation and control of technical and physical security measures.

Article 2b

1. The BIA conducts security checks of persons who are employed or who are to be employed at this security service, candidates for education and work at this security service, and other persons for whom this is required under this and other laws.
2. Security checks are also conducted of domestic and foreign natural persons and legal entities with which the BIA and another state authority and institution of national security importance plan to conclude a
contract on the purchase of goods and services or performance of works, under which the natural person or legal entity is granted access to secret data or protected persons or facilities in the way that can affect the security of the protected persons and facilities.

3. The BIA also conducts security checks of persons who are granted certificates for accessing data marked as “top secret” and “secret” in accordance with the law.

4. At the request of the competent police service, the BIA may also conduct security checks of persons who are being granted the Serbian citizenship and foreigners whose stay in the Republic of Serbia is of the national security importance.

5. The BIA may also conduct security checks of persons in other cases regulated by law, as well as for the needs of foreign security services and international organizations for the purpose of employment of these persons at foreign states’ authorities, or at international organizations, with the prior agreement of persons who are subjected to checks.

**Article 2v**

1. A person of whom a security check is performed under Article 2b paragraphs 1 through 3 of this Law fills in and signs a questionnaire with identification data. If the person does not sign the questionnaire, he/she will be considered to have withdrawn the application for employment or education and work, or given up the intention to conclude a contract, or withdrawn the request to obtain a certificate for access to secret data.

2. The purpose of a security check is to find out whether or not there are facts that prevent employment, admission to education and work, conclusion of a contract, or granting of a certificate for access to secret data (security impediment).

3. Within the security check, the authorized BIA representative may conduct an interview with the person who is being checked and, based on the latter’s written consent, conduct interviews with related persons, as well as collect the necessary data through operative activities. Data from official records belonging to other security services, authorities and institutions may be used in the procedure, on the basis of a written decision of the BIA director.

4. A written report is made on the results of the security check, and it is certified by the competent supervisor.

5. The person subjected to the security check is informed about its outcome, at his/her own request. If dissatisfied with the outcome of the check, the person is entitled to file a complaint to the BIA director and to receive a reply within 15 days from the date when the complaint was filed.

6. The method for conducting a security check is more closely regulated by a government regulation.

**Article 2g**

1. Data and records collected within security checks represent the data whose level of secrecy is determined in accordance with the regulations on confidential data.

2. Data and records referred to in paragraph 1 of this Article are protected in accordance with the regulations on personal data protection and may not be used for other purposes.

**Article 2d**

The BIA also performs the following activities:

1. Plans, organizes and implements the internal control of operation of its members;
2. Plans and organizes education, specialized courses and training of its members;
3. Protects the confidential data it collects and uses in its work;
4. Establishes archives and issues its own publications;
5. Secures and protects its members and facilities from unlawful acts and threats;
6. Protects the equipment and tools used in its operation from unauthorized access;
7. Plans its equipping and procures items for its own needs;
8. Performs other activities within its competence."

Article 3

Article 16 paragraphs 1 and 2 of the Law on the BIA are deleted.

3.2. Management and Internal Organization

Description of the Issue

In Articles 5 through 8, the Law on the BIA contains only basic, non-elaborated provisions on the management and internal organization of the BIA, which therefore do not ensure the appropriate legal certainty or legal guarantees required within the rule of law. Neither the existence of a deputy director, nor the procedure of his election have been regulated.

Possible Solution

These shortcomings can be removed by regulating in greater detail the conditions and procedures for the election of the BIA director and deputy director, their terms of office, method of adoption of a document on the internal organization and limitation of the director's authority for issuing operation instructions.

Proposed Amendments

Article 4

Article 5 of the Law on the BIA is amended as follows:

Article 5

9. The BIA is managed by the director, who is responsible for the lawful, professional, efficient and politically neutral operation of the BIA.
10. The BIA director is accountable to the government. The director has a deputy, who is accountable to the director and the government. The BIA director and deputy director are appointed and dismissed by the government.
11. The BIA director and deputy director are appointed to a five-year term of office.
12. Anybody who has at least nine years of experience in security and intelligence activities or other activities in the security sector may be appointed the BIA director and deputy director.
13. The government obtains the opinion on the candidates for the BIA director and deputy director from the president of the Republic, Council and National Assembly committee responsible for controlling security services."

Article 5

Article 6 of the Law on the BIA is amended as follows:
1. The BIA director issues a document on the internal organization and job classification and method of operation of the BIA, with the government’s agreement.
2. The document referred to in paragraph 1 of this Article is marked with the appropriate level of secrecy in accordance with the law regulating the secrecy of data.

In Article 8 of the Law on the BIA, new paragraph 2 is added, which reads as follows:

„Work instructions issued by the director must be in accordance with the Constitution, law, other regulation and general act, as well as with the security and intelligence policy of the Republic of Serbia."

3.3. Covert Measures

Description of the Issue

The Law on the BIA does not regulate covert measures that may be used in the implementation of operative methods, measures and activities and special measures for the covert collection of data, so that it remains legally unregulated whether, in which way and under which conditions covert measures are used in practice. As opposed to this, such measures are regulated in the Law on the VBA and VOA.

Possible Solution

In the Law on the BIA, after the provisions on special measures for the covert collection of data, provisions on the covert measures should be included, in order to give this issue its legal expression and thus ensure supervision over the implementation of these measures.

Proposed Amendments

After Article 15g of the Law on the BIA, Article 15d is added, which reads as follows:

1. In the implementation of operative measures, methods and activities and special measures referred to in Art. 9 and 13 of this Law, the BIA is authorized to use documents and means to conceal the identity of its members and natural persons with whom lasting cooperation has been established.
2. For the purposes referred to in paragraph 1 of this Article, the following IDs may not be used: those belonging to MPs, deputies and councilors, and those belonging to the members of the government, Secretariat-General of the government, Secretariat-General of the president and ombudsman, as well as the official IDs of judges, public prosecutors, members of other security services, police and other authorized official persons.
3. The BIA may also undertake measures to conceal the purpose of data collection, as well as use, against a consideration, secret services of natural persons and legal entities in the way and under the conditions defined in the BIA director’s act. The director issues this act after obtaining the opinion of the Council.

4. For the purposes referred to in paragraph 1 of this Article, the BIA may be allowed to use business and official premises owned by the Republic of Serbia, and it may have covert ownership of objects and legal entities.

5. Legal entities referred to in paragraph 4 of this Article may not be directly financed from the budget of the Republic of Serbia, autonomous province and local governance unit, and they perform activities and operate in accordance with relevant regulations.

6. The costs of the establishment and operation of legal entities referred to in paragraph 4 of this Article are borne by the BIA, from the budget item dedicated to special expenses. All the assets of these legal entities belong to the Republic of Serbia, and any revenues obtained through their business operation are used by the BIA as special-purpose funds. Data on the expenses and revenues are secret and subject to the control of the Council member appointed by the Council and control of the State Audit Institution.

7. The method and conditions for the use of authorizations referred to in paragraphs 4 through 6 of this Article are regulated by the government, upon obtaining the opinion of the Council.”

### 3.4. Control of Operation

**Description of the Issue**

Provisions on control in the Law on the BIA (Art. 17 through 19) regulate only the obligation to file semi-annual reports on operation and on the state of security to the National Assembly, obligation to comply with the general positions and guidelines of the government in the performance of activities and the obligation of persons who participate in the control of the BIA to protect and maintain the confidentiality of data and information obtained through control after the end of their term of office. This type of organization is obviously insufficient and needs to be expanded, independently from the fact that some issues of control, particularly by parliament, are regulated in greater detail under the ZOUSB.

**Possible Solution**

The Law on the BIA, in the chapter that regulates the control of operation, needs to include new provisions that would specify the obligation of filing special reports to the National Assembly as well as the obligation of establishing internal control and elements of the position and role of internal control.

**Proposed Amendments**

**Article 8**

A new paragraph is added to Article 17 of the Law on the BIA as paragraph 2, which reads as follows:

„The director is required to file a report on the BIA operation to the National Assembly committee responsible for controlling security services, both if necessary or at the request of the committee (special report).“
Article 9

Article 18 of the Law on the BIA is amended as follows:

Article 18

1. The BIA director is required to organize the internal control and appoint its supervisor.
2. The internal control supervisor is accountable to the BIA director and is required to file a report on the operation of the internal control, if necessary or at his request, as well as to report to him regularly and without delay on the results of control.
3. The internal control supervisor is required to notify the inspector-general of security services, and, if necessary, also the government, Council and National Assembly committee responsible for controlling security services about all cases in which he believes that the BIA director, in connection with the internal control results of which he has been notified, has failed to remove the unlawfulness or irregularity in operation, or other cases where he believes that the lawful and proper realization of the BIA activities has been seriously jeopardized.

3.5. BIA Members

Description of the Issue

In addition to the fact that they regulate a small number of issues and mostly make referrals to the implementation of regulations that apply on the employees in the ministry responsible for internal affairs, the provisions on BIA members (Art. 20 through 25) also have other shortcomings, such as, for example, the prohibition of organization in trade unions as well as the lack of regulation of some significant issues of importance for the specific position of the agency members.

Possible Solution

These issues can be overcome, at least as much as absolutely necessary, through amendments to the Law on the BIA. Interventions provided here tackle the key issues.

Proposed Amendments

Article 10

Article 20 of the Law on the BIA is amended as follows:

Article 20

1. BIA members are civil servants and state employees. The law and other regulations that apply on the employees of the ministry responsible for internal affairs also apply on their employment, rights and duties as well as termination of employment, unless this law and regulations adopted on its basis say otherwise.
2. Special criteria and procedure for the employment and termination of employment of BIA members are regulated by the government, at the proposal of the BIA director.
3. BIA members are prohibited to speak in public and to present data and knowledge about the operation of the BIA, as well as other data of security importance, without the agreement of the BIA director.
4. BIA members may be organized in trade unions and may establish professional associations within the BIA.
5. BIA members do not have the right to strike and may not be political party members.”

**Article 11**

Article 21 of the Law on the BIA is amended as follows:

**Article 21**

1. An authorized official person is a BIA member who may apply the legally regulated BIA authority while performing activities.
2. The BIA director defines which BIA members have the status of authorized official persons as well as the scope of their authority.
3. Authorized official persons of the BIA have official IDs with badges, while other BIA members only have official IDs.
4. The BIA director may grant some BIA members the status of persons at special duty, in accordance with regulations governing internal affairs.
5. The type, shape and content of the official ID and the appearance of the badge are regulated by the government, at the proposal of the BIA director.”

**Article 12**

In Article 22 of the Law on the BIA, after paragraph 2, paragraphs 3, 4 and 5 are added, and they read as follows:

„(3) Pripadnik BIA ne sme da izražava i zastupa svoja politička uverenja prilikom obavljanja službenih „(3) A BIA member may not express and promote his political beliefs during the discharge of official duties.
(4) If a BIA member believes that an order of the BIA director or his direct superior is unlawful, he is required to warn him thereof in writing, and if the superior still insists that the order be carried out, he is required to request a written confirmation of the order. If the order is confirmed, he is required to notify thereof the higher superior and internal control, or the government if the order was issued by the director.
(5) If a BIA member finds out about unlawful actions within the BIA, he is required to report this to the BIA director and internal control, without any consequences to his status. If the BIA director or internal control do not act upon the report, the BIA member may apply to the supervisory and control bodies, without any consequences to his status.”

**Article 13**

After Article 23 of the Law on the BIA, new Articles 23a, 23b and 23v are added and they read as follows:

**Article 23a**

A BIA member and a natural person with whom covert cooperation has been established may testify before judicial authorities in proceedings against persons suspected on the basis of BIA operations, only if the protection of their identity is ensured in accordance with this law, or the law regulating criminal procedure.
**Article 23b**

1. Under a document issued by the BIA director, a BIA member may be granted an additional coefficient on his salary, the value of which is determined by a government act.
2. The BIA may contract life insurance, insurance in the case of death or loss of work ability for its members, in accordance with risks related to the performance of activities.

**Article 23v**

A BIA member may be sent abroad within cooperation with another state’s security service or other corresponding agency, on the basis of an international agreement, or in accordance with the law.”

### 4. PROPOSALS FOR THE IMPROVEMENT OF THE LAW ON VBA AND VOA

#### 4.1. VBA Competences

**Description of the Issue**

Although the VBA competences are mostly determined in a detailed and proper manner under the Law on the VBA and VOA, the provisions on covert measures still need to be amended and the way for conducting security checks regulated, since these issues are currently not regulated fully. This would improve legal certainty within the operation of the agency and secure additional space for the needed more detailed control and legal protection of citizens who are subjected to security checks.

**Possible Solution**

The Law on the VBA and VOA should be amended in the same way as it has been proposed in the case of the Law on the BIA. There is a need to amend Article 22, as well as to introduce new provisions on security checks.

**Proposed Amendments**

**Article 1**

In Article 22 of the Law on the VBA and VOA, paragraphs 7, 8 and 9 are added after paragraph 6, and they read as follows:

“(7) The legal entity referred to in paragraph 6 of this Article may not be directly financed from the budget of the Republic of Serbia, autonomous province and local governance unit, and it performs activities and operates in accordance with relevant regulations.

(8) The expenses of establishment and operation of the legal entity referred to in paragraph 6 of this Article are borne by the VBA, from the budget item dedicated to special expenses. All assets of this legal entity
belong to the Republic of Serbia, and any revenue generated in its operation is used by the VBA as special-purpose funds. Data on its expenses and revenues are secret, and are controlled by the Council member who is appointed by the Council and by the State Audit Institution.

(9) The method and conditions for using competences referred to in paragraph 6 of this Article are regulated by the government, after obtaining the opinion of the Council.”

**Article 2**

After Article 22 of the Law on the VBA and VOA, Articles 22a and 22b are added, which read as follows:

**Article 22a**

1. A person subjected to a security check under Article 6 paragraph 1 item 5 and paragraph 4 item 7 of this Law fills out and signs a questionnaire on the identification data. If the person does not sign the questionnaire, he/she will be considered to have withdrawn the job application or the application for education and work, or given up the intention to conclude a contract or withdrawn the request to get a certificate for access to secret data.

2. The purpose of a security check is to find out whether or not there are facts that stand in the way of employment, admission for education and work, conclusion of a contract, or granting of a certificate for access to secret data (security impediment).

3. Within a security check, the authorized VBA member may conduct an interview with the person who is being checked and, on the basis of the latter’s written consent, conduct interviews with related persons and collect the necessary data through operative activities. Data from official records of other security services, authorities and institutions may be used in the procedure, on the basis of a written decision of the VBA director.

4. A written report is made on the results of the security check and it is certified by the competent manager.

5. The person who was subjected to the security check is notified about its outcome at his/her own request. If dissatisfied with the outcome, the person may complain to the VBA director and receive a response within 15 days from the date of filing of the complaint.

6. The way in which security checks are conducted is regulated in greater detail by a government regulation.

**Article 22b**

1. Data and records collected within security checks represent the data whose level of secrecy is determined in accordance with the regulations on confidential data.

2. Data and records referred to in paragraph 1 of this Article are protected in accordance with the regulations on personal data protection and may not be used for other purposes.”

### 4.2. VBA and VOA Management and Internal Organization

**Description of the Issue**

Article 37 of the Law on the VBA and VOA regulates the method of management, appointment of the director and deputy director of the VBA and VOA, as well as the conditions for their appointment. These conditions, however, refer only to persons who have completed the general staff specialization and who have at least nine years of experience in security and intelligence activities within the defense system (paragraph 6). In this way, persons with the same amount of experience on other positions in the security sector are eliminated as possible candidates for the positions of director and deputy director, which excessively narrows down the circle of potential candidates.
Possible Solution

Through an intervention in Article 37 paragraph 6 of the Law on the VBA and VOA, other candidates with the appropriate amount of experience in the security sector should be enabled to appear as candidates for the positions of director and deputy director of the VBA and VOA in the selection procedure.

Proposed Amendments

Article 3

In Article 37 paragraph 6 of the Law on the VBA and VOA, the period after the word „defense“ is deleted, a comma is inserted and the following words are added: „or a person with at least nine years of experience in the security sector“

4.3. Control of the VBA and VOA Operation

Description of the Issue

The Law on the VBA and VOA regulates the competences, position and other issues pertaining to the work of the inspector-general. In view of the fact that, according to the idea proposed herein, provisions on the Inspectorate-General would be contained in the ZOUSB, and since its mandate, in addition to the control of the VBA and VOA, would also include the control of the BIH and the Technical Operational Center, the provisions on the inspector-general would have to be deleted from the Law on the VBA and VOA.

Possible Solution

This is achieved through a provision on deleting the relevant provisions from the Law on the VBA and VOA.

Proposed Amendments

Article 4

Articles 54 and 55 of the Law on the VBA and VOA are deleted, as well as the provisions of Article 56 of the same Law in the part that refers to the inspector-general.