Časopis za poslovnu teoriju i praksu
The paper submitted: 05/05/2025
The paper accepted: 16/06/2025

UDK 342.738:]341.211:355.40
DOI 10.7251/POS2534165N
COBISS.RS-ID 142876673
Review

Novković Đorđe, Ministry of Interior of the Republic of Srpska, Police Administration Banja Luka, Bosnia and Herzegovina, djordje.novkovich@livecom

STATE SECRET – CONSPIRACY

Summary: *This paper provides a brief overview of confidentiality measures within the command chain of security agencies. It emphasizes the importance of adhering to organizational structures and command lines, particularly in communication centers and command posts, to prevent breaches of confidentiality. The paper also addresses the misuse of authority, where lower-level personnel assume roles with command rights, contradicting established protocols.*

Key words: *confidentiality, secrecy, command line, disclosure, penalties, countermeasures*

JEL classification: *K29*

INTRODUCTION

Secrecy and confidentiality are emphasized in all serious states as well as in the technical support for the leadership (command) staff, where Communication Centers and Cipher Units (KZ) cannot act on orders from lower organizational units due to organizational reasons and the risk of leaking official secrets up to the level of classified (state secret).
With the increasingly widespread use of information and communication technologies in correspondence between organizational units, confidentiality in everyday conversations of leaders and in planning operational actions has been neglected. This is evident in the fact that devices for photography and recording are brought into meeting rooms, offices, and Communication Centers and Cipher Units, which is strictly forbidden, as well as conversations about certain matters over mobile devices on public networks and correspondence via email (internet), bypassing the information security service organized as Communication Centers and Cipher Units.
In addition, this paper will address, besides the compromised secrecy workflow, the classification markings and the sanctions involved, as well as the breach of cryptographic personnel measures and the publication of such information online, all of which endanger the security policy in all serious security-intelligence and military organizations.

1. STATE SECRET – CONSPIRACY

1.1. State Secret – General Information

All data held by public authorities that have been justifiably and properly classified as secret are considered classified information (Horn 2012, 13). Classified data may include information related to the territorial integrity and sovereignty of the state, protection of the constitutional order, human and minority rights and freedoms, national and public security, internal and

external affairs, as well as foreign classified information (those entrusted to our state by foreign countries or international organizations, or created in cooperation with international entities). Protection is justified if disclosure would harm the work of a public authority or the interests of the state, provided that the protection of state interests outweighs the public's right to access information of public importance.
Additionally, under the secrecy law, data marked as secret that cover a criminal offense, abuse of authority, misuse of official position, or other illegal acts are not considered secret. Unfortunately, this does not mean that some authorities will not try to withhold such information. However, if you obtain or become aware of such a document, you should contact the Commissioner for Access to Public Information, who can request the removal of the secrecy classification. If you publish such a document without this procedure, you may have to prove in court that the document did not meet the conditions for classification as secret.

1.2. Levels of Confidentiality

The term "state secret" often encompasses all information the state wishes to conceal. However, it specifically refers to the highest level of secrecy. The classification levels are as follows:

1. INTERNAL: Documents that misuse could disrupt the functioning of a public authority.
2. CONFIDENTIAL: Documents that misuse could harm state interests.
3. STRICTLY CONFIDENTIAL: Documents that misuse could cause significant harm to state interests.
4. STATE SECRET: Documents that misuse could cause irreparable severe harm to state interests.

Unauthorized access to these categories can lead to varying legal consequences.

1.3. Document Classification

Only authorized individuals, such as the President of the National Assembly, the President of the State, the Prime Minister, heads of public authorities, or officials authorized by law, can designate information as secret.
The duration of secrecy can be time-limited or event-based. If not specified, the secrecy duration is determined by the classification level, with each level having a set number of years. A secret ceases to be classified when it becomes publicly known, regardless of the reason.
Each document containing classified information must be visibly marked. The marking must include the classification level ("internal", "confidential", etc.). In addition to the classification level, it will usually include the declassification method (a specific event or fact leading to declassification), information about the authorized person, and information about the public authority that declared the data classified.

2. BASIC PROVISIONS ON CLASSIFICATION

The basic provisions regulate a unified system for the classification and protection of classified information that is of interest to national and public security, defense, internal and foreign affairs of the state, protection of foreign classified information (Aistrope and Bleiker 2018, 169), access to classified data and termination of their classification, the competence of authorities, supervision over the implementation of this law (Humayun 2013, 107), as well as liability for non-compliance with this law and other issues relevant to data secrecy protection and definitions.

1. Information of state interest is any information or document held by a public authority concerning territorial integrity and sovereignty, constitutional order, human and minority rights and freedoms, national and public security, defense, internal and foreign affairs.

2. Classified information is information of state interest designated and marked with a certain level of classification by law, other regulation, or decision of a competent authority made in accordance with the law.
3. Foreign classified information is information entrusted to the state by a foreign state or international organization under the obligation to protect it as classified, as well as classified data created in cooperation with other states, international organizations, or other international entities in accordance with a concluded international agreement.
4. A document is any data carrier (paper, magnetic or optical medium, diskette, USB drive, smart card, CD, microfilm, video or audio recording, etc.) containing or storing classified information.
5. Classification of information is the procedure of designating information as classified, determining the level and duration of classification in accordance with this law.
6. Marking the classification level means labeling classified data with one of the following: "state secret", "top secret", "confidential", or "internal".
7. Public authority includes state bodies, bodies of territorial autonomy, local self-government, organizations with public authority, and legal entities established or funded predominantly by the state budget that handle classified information.
8. Security check is a procedure conducted by a competent authority before issuing clearance for access to classified data to determine potential security risks.
9. Damage refers to harm to the state's interests resulting from unauthorized access, disclosure, destruction, or misuse of classified or foreign classified data.
10. Data handler is an individual or organizational unit within a public authority that applies protection measures for classified information under this law.
11. Data user is a citizen or legal entity based in the country with a permit issued by a competent authority, or a foreign person or entity with security clearance based on an international agreement.
12. Security risk is a real possibility of compromising the security of classified information.
13. Protection measures include general and specific administrative, IT and telecommunications, personnel, and physical security measures.

2.1. Data Not Considered Classified

Information is **not considered classified** if marked as such to conceal a criminal offense, abuse of power, or other unlawful acts or misconduct by public authorities.

2.2. Right of Access

Access to classified information is granted under the conditions and procedures established by this law, accompanying regulations, and international agreements.

2.3. Purpose of Collection

Classified data may be used only for the purpose for which it was collected, in accordance with the law.

2.4. Storage and Use

Classified data must be stored and used according to protection measures prescribed by law, bylaws, and international agreements.
Anyone using or acquainted with the content of classified data is obligated to maintain confidentiality, regardless of how they learned the information.
This obligation continues even after termination of employment, office, or public function.

3. CLASSIFICATION OF INFORMATION

Data That May Be Classified
Data of state interest may be classified if its disclosure to unauthorized persons would cause harm, and if protecting such data outweighs the public's right to access information.
This applies to:

1. National or public security, defense, foreign policy, intelligence matters;
2. Relations with other states or international organizations;
3. Systems, devices, plans, or structures;
4. Scientific, research, technological, economic, and financial operations.

3.1. Authorized Persons for Classification

The following may classify information:

1. The President of the Republic;
2. The Speaker of the Parliament;
3. The Prime Minister;
4. The head of a public authority;
5. An elected, appointed, or designated official of a public authority who is authorized by law or a regulation adopted pursuant to law to classify information, or who has been formally authorized in writing by the head of the public authority;
6. An employee of a public authority who has been formally authorized in writing by the head of that authority.

3.2. Classification Procedure

The authorized person shall determine the classification of information at the time of its creation, that is, when a public authority begins work that will result in the creation of classified information.
Exceptionally, the authorized person may also determine the classification retroactively, once the criteria set by this law have been met.
When classifying information, the authorized person shall assess the potential damage to the interests of the state.
An employee or person performing certain tasks within a public authority is obligated, within the scope of their duties or authority, to inform the authorized person on any data that may need to be classified.

3.3. Decision on Classification Level

The decision to assign a classification level to information is made based on an assessment, and accordingly, the document is marked with a classification label (hereinafter: classification marking).
When determining the classification level of information, the authorized person shall assign the lowest level of classification necessary to prevent harm to the interests of the state.
If the document contains information that could be assigned different classification levels, the authorized person shall mark the document with the highest applicable classification level.

3.4. Special Cases of Classification

An authorized person shall classify as secret any information that arises from the aggregation or correlation of data, which, individually, are not classified, if the combined or related information constitutes classified data that must be protected for reasons defined by this law.

A document containing information already classified under different levels and retention periods shall be marked according to the highest classification level and the longest retention period applicable to any part of its content.
If a minor portion of a document contains classified information, it shall be separated and attached to the document as a distinct annex, marked with the appropriate classification label.

3.4.1. Marking Classified Documents

Documents with classified content must include:
1. Classification level;
2. Declassification method;
3. Authorized person details;
4. Public authority details.

A document containing classified information shall be considered classified only if it is marked with a classification level**,** in accordance with the procedure and method prescribed by the Government for labeling classified data or documents.

3.4.2. Classification Levels

1. "STATE SECRET"**,** which is assigned to prevent the occurrence of irreparable and severe harm to the interests of the state;
2. "TOP SECRET"**,** which is assigned to prevent the occurrence of severe harm to the interests of the Republic of Serbia;
3. "CONFIDENTIAL"**,** which is assigned to prevent the occurrence of harm to the interests of the Republic of Serbia;
4. "INTERNAL"**,** which is assigned to prevent the occurrence of harm to the functioning or performance of tasks and duties of the public authority that designated the data.

Only the classification levels listed in paragraph 1 of this Article may be applied when assigning classification levels to data. The Government shall determine detailed criteria for assigning the classification levels "STATE SECRET" and "TOP SECRET", **based on the prior opinion** of the competent ministry or agency. The criteria for assigning "CONFIDENTIAL" and "INTERNAL" shall be determined by the Government upon the proposal of the competent minister **or the** head of the public authority**.**

3.4.3. Marking Foreign Classified Information

A document containing foreign classified information shall retain the classification level assigned by the foreign state or international organization.
When marking the classification level of documents intended for cooperation with foreign states, international organization**s**, or other subjects of international law, classification labels in English may be used**,** in addition to local terminology, as follows:
1. The label **"**TOP SECRET" corresponds to the classification level **"**STATE SECRET";
2. The label "SECRET" corresponds to the classification level "TOP SECRET" (in Serbian: *"STROGO POVJERLjIVO"*);
3. The label "CONFIDENTIAL" corresponds to the classification level "CONFIDENTIAL" (*"POVJERLjIVO"*);
4. The label "RESTRICTED" corresponds to the classification level "INTERNAL" (*"INTERNO"*).

4. DECLASSIFICATION

4.1. Time Limitations

The confidentiality of data shall cease:

1. on the date specified in the document containing the classified information;
2. upon the occurrence of a specific event specified in the document containing the classified information;
3. upon expiration of the legally prescribed period;
4. upon revocation of the classification;
5. if the information has been made publicly available.

An authorized person may change the method prescribed for the termination of the classification of the information, if there are justified reasons to do so, in accordance with the law.

The authorized person is obliged to notify, without delay and in writing, the public authorities and persons who have received or have access to the classified information about such a change.

4.2. Declassification by Date

If the authorized person, during the process of determining classification, establishes that the reasons for classifying the information cease upon the occurrence of a certain date, they shall determine the date of declassification and mark it in the document containing such information.

4.3. Termination of Classification upon the Occurrence of a Certain Event

If the authorized person, in the process of determining classification, establishes that the reasons for classifying the information cease upon the occurrence of a certain event, they shall determine that the classification ends upon the occurrence of that event and mark it in the document containing such information.

4.4. Termination of Classification by Expiry of the Period

If the termination of classification of the information is not specified, the classification ends upon expiry of the period determined by law regulating that area.
The statutory period for termination of classification of information from paragraph 1 of this article is determined according to the classification level, as follows:

1. For information marked “STATE SECRET” - 30 years;
2. For information marked “STRICTLY CONFIDENTIAL” - 15 years;
3. For information marked “CONFIDENTIAL” - 5 years;
4. For information marked “INTERNAL” - 2 years.
   The periods run from the date the information was classified.

5. EXTENSION OF THE CLASSIFICATION PERIOD

5.1. Extension of the Period of Classification

If, after the expiry of the period, there are reasons for the information to remain classified, the authorized person may extend the period for termination of classification for a maximum duration determined for each classification level.

In addition to the authorized person, the Government may extend the classification period in cases when:

1. Its disclosure would cause irreparable severe harmful consequences to national security and especially vital state, political, economic, or military interests of the state;

2. It is provided for by an international agreement or other international obligations;
3. Its disclosure would cause irreparable severe consequences to the fundamental human and civil rights of one or more persons, or would endanger the security of one or more persons.

6. REVOCATION OF CLASSIFICATION

6.1. Revocation of Classification of Information

In the process of revoking classification, it is established that the information ceases to be classified before the expiry of the classification period.
The decision to revoke classification is made if facts and circumstances arise due to which the information ceases to be of interest to the state.
Periodic Review of Classification.
The authorized person conducts periodic reviews of classification, based on which they may revoke classification, as follows:

1. For information marked "STATE SECRET", at least once every ten years;
2. For information marked "STRICTLY CONFIDENTIAL", at least once every five years;
3. For information marked "CONFIDENTIAL", at least once every three years;
4. For information marked "INTERNAL", at least once every year.

If reasons for revocation are established, the authorized person promptly issues a reasoned decision on revocation.

6.2. Proposal for Revocation of Classification

The user of the classified information may propose revocation of classification to the authorized person.
The authorized person is obliged to consider the proposal from paragraph 1 of this article and notify the proposer of their decision.

6.3. Revocation of Classification in the Process of Control

During the process of control for national security and protection of classified information, an extraordinary classification review of information can be requested from the authorized person, who may then independently decide on revocation of classification based on that review.

6.4. Revocation of Classification Based on Decision of a Competent Authority

The authorized person of the public authority revokes the classification of information or documents containing classified information and enables the exercising of rights by the requester or applicant based on a decision of the Commissioner for Information of Public Importance and Personal Data Protection in appeal proceedings, or based on a decision of the competent court in litigation, in accordance with laws regulating free access to public information and personal data protection.

6.5. Revocation of Classification in the Public Interest

The National Assembly, the President of the Republic, and the Government may revoke the classification marking from certain documents, regardless of classification level, if it is in the public interest or due to fulfillment of international obligations.

6.6. Change of Classification Level and Duration of Classification

Notification of change in classification level and revocation of classification — the authorized person shall promptly notify in writing the users of classified information or persons with access to such information about changes in classification level, duration, or revocation of classification.
Foreign Classified Information.
Changes to classification level and period, as well as revocation of classification of foreign classified information, are carried out in accordance with concluded international agreements and established international obligations.

7. MEASURES FOR THE PROTECTION OF CLASSIFIED INFORMATION

Criteria for Protection of Classified Information.
Public authorities establish a system of procedures and protective measures according to the following criteria:

1. Level of classification;
2. Nature of the document containing the classified information;
3. Threat assessment to the security of the classified information.

7.1 Types of Protective Measures

Public authorities apply general and special protective measures pursuant to the law and regulations, to protect classified information in their possession.

7.1.1 General Protective Measures

General Protective Measures include:

1. Determining the level of classification;
2. Assessing threats to the security of classified information;
3. Defining how to use and handle classified information;
4. Designating responsible persons for safeguarding, using, exchanging, and processing classified data;
5. Appointing the information handler, including security clearance depending on classification level;
6. Designating special zones, buildings, and rooms for protection of classified and foreign classified information;
7. Monitoring handling of classified data;
8. Physical and technical protection measures including installation of security devices and zones;
9. Protection of information and telecommunication systems;
10. Cryptographic protection measures;
11. Protective regime for workplaces and organizational posts;
12. Special education and training programs for classified information protection;
13. Other general measures prescribed by law.

7.1.2 Special Protective Measures

Special measures supplement general ones to enhance security. Acts of the competent minister or head of a special organization, per government directives, may further regulate them.

7.2 Obligations of the Information Handler

The handler of classified information undertakes protective measures, grants user direct access, issues copies of documents containing classified data, keeps records of users, and manages exchange of classified information.

7.3 Storage, Transfer, and Delivery of Classified Information

Classified Information Handling and Incident Reporting.
Classified information must be stored in a manner that ensures access is granted only to authorized users. Transmission and delivery of classified information outside the premises of public authorities are allowed only when prescribed security measures and procedures are followed, ensuring that the information is received solely by individuals who possess the appropriate clearance (certificate) and have the right to access such data. The procedures and protective measures applied during the transmission and delivery of classified information must correspond to the classification level of the information, in accordance with the law and relevant regulations.
When classified information is transmitted or delivered using telecommunication or information technologies, the application of legally prescribed cryptographic protection measures is mandatory. The implementation of cryptographic protection measures during the transmission and delivery of classified information must be conducted in accordance with the law.
Duty to Report Security Incidents.
In the event of loss, theft, damage, destruction, or unauthorized disclosure of classified or foreign classified information, any official, employee, or individual performing duties within a public authority must immediately notify the authorized officer of the public authority upon becoming aware of such an incident (Đorđević 2017, 221).
Any individual who determines that classified or foreign classified information has been lost, stolen, damaged, destroyed, or disclosed without authorization during transmission or delivery outside the premises of the public authority must immediately inform the authorized officer of the authority that transmitted or delivered the classified information.
The authorized officer is obligated to promptly take all necessary actions to determine the circumstances of the incident, assess the resulting damage, and implement appropriate measures to eliminate the damage and prevent recurrence of such incidents involving the loss, theft, damage, destruction, or unauthorized disclosure of classified or foreign classified information.

8. ACCESS TO CLASSIFIED INFORMATION

Access to classified information without a certificate.
The Speaker of the National Assembly, the President of the Republic, and the Prime Minister have the right to access and use classified information and documents of any classification level without the issuance of a certificate, based on their function and for the purpose of performing duties within their jurisdiction.
Access to classified information without security clearance and special authorizations and duties
State bodies appointed by the National Assembly, heads of state bodies appointed by the National Assembly, Constitutional Court judges, and judges are authorized to access information of all classification levels necessary for performing their duties without security clearance.
Exceptionally, individuals have the right to access classified information marked as “STATE SECRET” and “STRICTLY CONFIDENTIAL” after prior security clearance, if necessary for performing duties within their jurisdiction, when such information relates to:

1. actions to prevent, detect, investigate, and prosecute criminal offenses carried out by competent state authorities until the conclusion of the investigation or prosecution;
2. methods of applying special procedures and measures in obtaining security and intelligence data in a specific case;
3. members of the Ministry responsible for internal affairs and security services with concealed identities, when necessary to protect the vital interests of these persons or their family members (life, health, and physical integrity);
4. the identity of current and former collaborators of security services, or third parties, when necessary to protect the vital interests of these persons or their family members (life, health, and physical integrity).

Persons who have access to classified information pursuant to this law are authorized and obligated to protect the confidentiality of the information they learn during proceedings or otherwise, by all appropriate means, and to personally access classified information.
Right of access to classified information for members of the relevant committee of the National Assembly.
Members of the National Assembly committee responsible for oversight and control in the defense and security sector have the right to access and review classified information related to the performance of their oversight and control function, in accordance with the law.
Right of access to classified information marked as "INTERNAL" Officials, employed persons, or persons performing tasks in public authorities have access to classified information marked with the classification level "INTERNAL."
Access to foreign classified information.
Access to foreign classified information is carried out in accordance with this law, regulations adopted based on this law, or in accordance with an international agreement concluded by the state with a foreign country, international organization, or other international subject.

8.1. Natural and legal persons as users of classified information

A natural or legal person – a user of classified information – has the right to access classified information necessary for performing duties within the scope of their work and classified according to the level indicated in the certificate for access to classified information (hereinafter: certificate), or permit.
Exceptionally, in urgent cases, a person who has been issued a certificate or permit to access classified information marked with a lower classification level may be informed of classified information marked with the immediately higher classification level.
The person referred to in paragraph 2 of this article is obliged to sign a statement confirming that they will handle classified information in accordance with the law and other regulations.

8.2. Statement and decision

Before issuing the decision or permit, the person to whom the decision is issued is required to sign a statement confirming that they will handle classified information in accordance with the law and other regulations. If the person does not sign the statement, the procedure for issuing the decision or permit is suspended. The written statement is an integral part of the documentation based on which the decision or permit is issued.

8.3. Release from the duty to maintain secrecy

The person to whom the decision or permit is issued cannot use the information for purposes other than those for which the decision or permit was issued.
The head of the public authority may, at the request of the competent authority, release the person from the duty to maintain the secrecy of information by a special decision which will

also specify measures for the protection of classified information, but only for the purposes and scope contained in the request of the competent authority, in accordance with the law. At the request of the competent authority, the head of the public authority may be released from the duty to maintain the secrecy of information by the body that appointed, elected, or designated them.

8.4. Delivery of classified information with an obligation to maintain secrecy

Classified information may be delivered to another public authority based on a written approval of an authorized person of the public authority that classified the information, unless otherwise stipulated by special law.

Classified information obtained from a public authority cannot be delivered to another user without the consent of the authority that classified the information, unless otherwise provided by special law.

Persons performing tasks in a public authority to which classified information has been delivered are obliged to act in accordance with the provisions of this law, respecting the classification marking and taking measures to protect the confidentiality of the information.

8.5. Delivery of classified information based on a contractual relationship

An authorized person may deliver classified information to other legal or natural persons who provide services to the public authority based on a contractual relationship, if:

1. the legal or natural person meets the organizational and technical conditions for protecting classified information in accordance with this law and regulations adopted on the basis of this law;
2. security clearances have been conducted, and certificates issued for persons performing the contracted tasks;
3. persons referred to in point 2 of this paragraph have signed a written statement confirming that they are familiar with this law and other regulations governing the protection of classified information and undertake to handle classified information in accordance with those regulations;
4. access to classified information is necessary for the realization of the tasks provided by the contract.

Measures for the protection of classified information arising from paragraph 1 of this article must be contained in the contract concluded between the public authority and the legal or natural person regarding the realization of tasks.

The Government shall regulate in detail the manner and procedure for determining the fulfillment of security clearance requirements.

9. PROCEDURE FOR ISSUING DECISIONS OR PERMITS

9.1. Conditions for issuing a decision to a natural person

A decision is issued by the competent authority established by this law, based on a written request from a natural person, if the applicant:

1. is a citizen of a country;
2. is of legal age;
3. is legally competent;
4. has not been convicted of an unconditional prison sentence for a criminal offense prosecuted ex officio, or for an offense prescribed by this law;
5. has passed the appropriate security clearance.

9.2. Conditions for issuing a decision to a legal entity

A certificate is issued by the competent authority established by this law, based on a written request from a legal entity submitted through its legal representative, if the applicant:

1. has a registered seat within the territory of the Republic;
2. performs activities related to the interests defined in the relevant articles;
3. passes the appropriate security clearance;
4. is not undergoing liquidation or bankruptcy proceedings;
5. has not been sanctioned by a prohibition to perform activities, or been subject to a sanction terminating the legal entity or prohibiting performance of certain registered activities or tasks;
6. pays taxes and contributions properly.

9.3. Issuance of permits to foreign persons

The competent authority issues a permit to a foreign person if:

1. they possess a valid security certificate issued by the state of which they are a citizen, or where they have their seat, or by an international organization of which they are a member;
2. the obligation to enable access to classified information arises from an international agreement concluded.

9.4. Submission of requests

Requests for issuing decisions or permits are submitted to the Ministry of Security. If the permit is requested by a manager or another employee of a public authority, the request is submitted through the head of that public authority.
If the decision is requested for a legal entity and its employees, the request is submitted by the legal representative of the legal entity.
Requests for issuing decisions to persons who will have access to classified information related to the performance of contracted work with a public authority are submitted by the relevant public authority responsible for the contracted work.

9.5. Contents of the request

A request from a natural person for a decision contains: full name, residence, work performed, reasons for requesting the certificate, and the classification level of information for which the certificate is requested.
A request from a legal entity contains: the name of the company, seat and activity of the legal entity, full name and residence of the legal representative of the legal entity, reasons for requesting the decision, and the classification level of information for which the decision is requested.

9.6. Security clearance

Security clearance for access and use of classified information is performed depending on the classification level, as follows:

1. Basic security clearance, for information classified as “INTERNAL” and “CONFIDENTIAL”;
2. Complete security clearance, for information classified as “STRICTLY CONFIDENTIAL”;
3. Special security clearance, for information classified as “STATE SECRET”.

9.7. Authority responsible for conducting security clearance

Security clearance for access to classified information and documents classified as "STATE SECRET" and "STRICTLY CONFIDENTIAL" is conducted by the Intelligence Service. Security clearance for access to classified information and documents classified as "CONFIDENTIAL" and "INTERNAL" is conducted by the ministry responsible for internal affairs.
Security clearance for access to classified information and documents of all classification levels for persons requiring access due to their functions or duties in the ministry responsible for defense and the Army is conducted by the Military Security Service.
Exceptionally, security clearance for access to classified information and documents classified as "CONFIDENTIAL" and "INTERNAL" for persons requiring access due to their functions or duties in the Security-Intelligence Agency is conducted by the Security-Intelligence Agency itself.
Security clearance for access to classified information and documents classified as "STRICTLY CONFIDENTIAL" for persons requiring access due to their functions or duties in the ministry responsible for internal affairs is conducted not only by the competent authority but also by the ministry responsible for internal affairs.
Authorities responsible for security clearance are obliged to cooperate mutually during the clearance procedure, especially regarding clearance for access to information classified as "STATE SECRET" and "STRICTLY CONFIDENTIAL."

9.8. Cooperation with foreign states and international organizations

Authorities responsible for security clearance may cooperate in the security clearance procedure with authorities of foreign states, international organizations, and other international entities responsible for security clearance, in accordance with international agreements concluded with the foreign state, international organization, or other international entity (Dentith and Orr 2018, 166).

9.9. Purpose of the security clearance

A security risk assessment is conducted for the applicant, especially regarding access to and use of classified information (Olmsted 2011, 98).
Within the security clearance, the competent authority evaluates the statements in the completed security questionnaire from a security perspective.
The competent authority collects personal and other data related to the applicant from the individual concerned, other public authorities, organizations, and persons, as well as from registries, records, files, and data collections maintained under the law.

9.10. Security questionnaire

For conducting the security clearance, the Council Office provides the security questionnaire to the applicant.
The applicant completes the basic security questionnaire, and if a certificate is requested for classified information of the "STATE SECRET" or "STRICTLY CONFIDENTIAL" level, a special security questionnaire must also be completed.
The completed and signed questionnaire submitted by the applicant simultaneously represents written consent for conducting the security clearance and is classified as "INTERNAL".

9.10.1. Basic security questionnaire for natural persons

The following data about the applicant are entered in the basic security questionnaire:

1. full name, including previous names and surnames;
2. unique citizen identification number;
3. date and place of birth;
4. citizenship, previous citizenships, and dual citizenships;
5. residence and domicile, including previous residences;
6. marital and family status;
7. data on persons living in the same household with the applicant (their full names, including previous names, dates of birth, and relation to the applicant);
8. full name, date of birth, and residence address of relatives up to the second degree in the direct line and first degree in the collateral line, adopters, guardians, stepfathers, stepmothers, or foster parents;
9. educational background and occupation;
10. data on previous employments;
11. data related to military service;
12. data on criminal and misdemeanor punishments and ongoing criminal or misdemeanor proceedings;
13. medical data related to illnesses involving dependencies (alcohol, narcotics, etc.) or mental illnesses;
14. contacts with foreign security and intelligence services;
15. disciplinary proceedings and measures imposed;
16. data on membership or participation in activities of organizations whose activities or goals are prohibited;
17. data on responsibility for violations of regulations related to secrecy of information;
18. data on ownership or other real rights on real estate, ownership data on other assets registered in public registers, and data on the annual personal income tax for the previous year;
19. previous security clearances.

9.10.2. Basic security questionnaire for legal entities

The following data about the applicant are entered in the basic security questionnaire for legal entities:

1. company name and seat, including previous company names and seats;
2. registration number and tax identification number;
3. full name of the representative;
4. date and place of establishment;
5. data on organizational units, branches, subsidiaries, and other forms of association;
6. origin of founding capital including changes in the last three years;
7. number of employees;
8. number of employees for whom the certificate is requested and types of work performed;
9. data on convictions for criminal offenses, economic offenses, and misdemeanors of the legal entity and responsible persons, as well as ongoing proceedings for criminal offenses, economic offenses, or misdemeanors against the legal entity;
10. data on contacts with foreign security and intelligence services;
11. data on participation in activities of organizations whose activities and goals are prohibited;
12. data on responsibility for violations of regulations related to secrecy of information;
13. data on previous security clearances;

14. data on ownership or other real rights on real estate, ownership data on other assets registered in public registers, and data on the annual financial report for the previous year, in accordance with laws regulating accounting and auditing.

Along with the completed questionnaire, the legal entity's representative also submits the completed basic security questionnaire for the natural person.

9.10.3. Special security questionnaire

For security clearance prescribed by law, in addition to the basic questionnaire, a special security questionnaire is completed.

The special security questionnaire includes data on:

1. service in foreign armies and paramilitary formations;
2. other data and facts that make the natural or legal person susceptible to influences and pressures representing a security risk;
3. debts incurred due to financial obligations or assumed guarantees.

9.10.4. Special security clearance

The special security clearance is conducted when the issuance of a decision or permit is requested for information classified as “STATE SECRET”.

The special security clearance includes, in addition to fact-checking within the complete security clearance, verification of facts, circumstances, and events from the applicant's private life for at least the last ten years from the date of submitting the request, which could raise doubts about their trustworthiness and reliability, especially if their activities conflict with the interests of the state or if they are connected with foreign persons who could endanger the security and international interests of the state.

9.11. Deadline for conducting the security clearance

The competent authority must conduct the security clearance within the following deadlines from the date the questionnaire is completed:

1. up to 30 days for basic security clearance;
2. up to 60 days for complete security clearance;
3. up to 90 days for special security clearance.

Exceptionally, if justified reasons exist, these deadlines may be extended for the maximum periods defined above.

If the competent authority grants an extension, it must notify the head of the public authority who submitted the security clearance request.

If the security clearance is not conducted within these deadlines, it is considered that there is no security risk related to the applicant's access to classified information.

9.12. Temporary decision

To carry out urgent tasks of the public authority and to prevent or eliminate damage, the director of the security agency may exceptionally issue a temporary decision for access to certain classified information before the completion of the security clearance, if, based on the review of the submitted security questionnaire, no security doubts are identified.

The person must confirm by written statement that they will handle the entrusted classified information in accordance with this law and other regulations governing the protection and handling of classified information.

The temporary decision is valid until the completion of the certification issuance procedure.

9.13. Submission of the report on security clearance results

Authorities responsible for conducting the security clearance, in accordance with laws, submit a report on the results of the security clearance, including the special security clearance and the completed security questionnaire, with a recommendation for issuing or denying the decision to the relevant authority.
The report and recommendation are classified as "CONFIDENTIAL".

9.14. Decision and supplementary verification

If the report is incomplete or submitted without a recommendation, a decision is made based on the submitted report.
Exceptionally, if from the results of the security clearance and the recommendation it cannot be determined whether the legal conditions for issuing the decision to the natural or legal person are met, or if after the security clearance there is a significant change in the verified data that could affect the issuance of the decision, the Agency will request the competent authority to perform supplementary verification, update the report, and prepare a new recommendation within an additional 30-day period.

9.15. Exceptions

For persons who need access to classified information due to performing functions or work duties in state security services, the decision to issue a clearance for access to classified information held by the security service is made by the head of the service.

9.16. Delivery of the Decision

The Agency delivers the decision to the head of the public authority that requested the issuance of the decision and to the person for whom the clearance was requested.

9.17. Rejection of the Request

The Agency rejects the request for issuance of clearance by decision if, based on the report of the security or supplementary security check, it is established that:

1. the applicant provided false or incomplete data in the basic or special security questionnaire;
2. the applicant does not meet the conditions for issuing clearance;
3. the applicant has not ensured the conditions for undertaking prescribed protective measures for classified information;
4. there is a security risk in granting access to and using the classified information by the applicant.

The reasoning of the decision rejecting the issuance of clearance does not contain data considered classified under this law, nor does it disclose the sources of the security check.

9.18. Content, Form, and Delivery of the Decision

The content, form, and method of delivering the certificate are prescribed by the Government, which also issues the clearance and informs the user of the prescribed conditions for handling classified information, as well as the legal and other consequences of unauthorized use.
When receiving the certificate, the user signs the certificate and a statement that they are familiar with the provisions of this law and other regulations governing the protection of

classified information and that they will use classified information in accordance with the law and other regulations.

9.19. Termination of Validity of the Decision

The clearance ceases to be valid:

1. upon expiration of the time for which it was issued;
2. upon termination of the person's function;
3. upon termination of performing duties and tasks within the scope of the person's work;
4. based on the Agency's decision made during the verification procedure of the issued decision;
5. upon the death of the natural person or termination of the legal entity to whom the clearance was issued.

9.20. Expiry of the Certificate by Time

A certificate issued for information and documents marked with the secrecy level "STATE SECRET" is valid for three years.
A certificate issued for information and documents marked with the secrecy level "STRICTLY CONFIDENTIAL" is valid for five years.
A certificate issued for information and documents marked with the secrecy level "CONFIDENTIAL" is valid for ten years.
A decision issued for information and documents marked with the secrecy level "INTERNAL" is valid for 15 years.

9.21. Extension of Validity of the Decision

The Agency notifies the holder of the certificate in writing that they may submit a request for extension of the certificate validity no later than 6 months before the expiration of the validity of the decision.
With the request for extension, the applicant informs the Agency about all changes to the data from the previously submitted security questionnaire with evidence and undergoes a new security check.

9.22. Temporary Prohibition of Access Rights

If disciplinary proceedings are initiated against a person issued a certificate due to serious violation of official duties, serious violation of military discipline, or serious breach of work obligations and duties, criminal proceedings for a justified suspicion of committing a criminal offense prosecuted ex officio, or misdemeanor proceedings for a misdemeanor provided by this law, the head of the public authority may temporarily prohibit access to classified information for that person until the final conclusion of the proceedings.

9.23. Verification of the Decision

If it is determined that the person to whom the certificate was issued does not use or protect classified information in accordance with this law and other regulations, or no longer meets the conditions for issuance of the certificate, the Office of the Council issues a decision on the termination of the certificate validity or on the expiration of the validity period, or a decision on restricting the right of access to classified information marked with a certain level of secrecy. The reasoning of the decision does not contain data considered classified under this law.

The decision of the Office of the Council is final and may be contested by administrative dispute.

9.24. Issuance of Clearance to Foreign Persons

The Agency issues clearance to foreign persons in accordance with an international agreement concluded.
Upon receiving the request, the Agency, through international exchange, verifies whether the applicant has been issued a security certificate by the state of which they are a citizen or in which they have their seat, or by the international organization of which they are a member.
The clearance is issued only for access to data and documents specified in the concluded international agreement that the state has signed with the foreign state, international organization, or other international entity.
Provisions of this law regarding issuance of decisions apply accordingly to the issuance of clearance to foreign persons.

9.25. Official Records and Other Data Related to Decisions and Clearances

The Agency maintains a unified central registry of issued certificates and clearances, decisions on issuing certificates and clearances, decisions rejecting issuance of certificates and clearances, decisions extending validity of certificates and clearances, and decisions restricting or terminating the validity of certificates and clearances, as well as signed statements of persons to whom certificates or clearances were issued.
The Agency keeps requests for issuance of certificates or clearances, security questionnaires, and reports on security checks with recommendations.

9.26. Registry of Security Checks

The authority responsible for conducting security checks maintains records of security checks and keeps documents related to the security check with copies of reports and recommendations.
Data from security checks may be used only for the purposes for which they were collected.

9.27. Application of Personal Data Protection Regulations

Regarding data from their security check collected under this law, the person has the right of access and other rights based on the right of access in accordance with the law regulating the protection of personal data, except for data that would reveal methods and procedures used in data collection, as well as identify sources of data from the security check.

9.28. Registry of Public Authorities

A public authority keeps records of decisions on certificates for persons performing functions or employed in the public authority or performing tasks.
Decisions on issued clearances for persons are kept in a special part of the personnel file, and data from the decision may be used only in connection with the implementation of provisions of this law or regulations enacted based on this law.
A detailed regulation on the content, form, and manner of keeping records is carried out by Internal Control.
The head of the public authority is responsible for internal control over the implementation of this law and regulations enacted based on this law.
In the ministry responsible for internal affairs, the ministry responsible for defense, and the Security-Intelligence Agency, and if necessary in other public authorities, a special position is

systematized for internal control and other expert tasks related to the determination and protection of classified information, or an existing organizational unit within the ministry or agency is specifically assigned these tasks.

9.29. Purpose of Internal Control

Internal control ensures regular monitoring and evaluation of individual activities, as well as the activity of the public authority as a whole, regarding the implementation of this law and regulations and measures adopted based on this law.
The head of the public authority, directly or through an authorized person, conducts internal control by direct inspection, appropriate checks, and consideration of submitted reports.

9.30. Taking over Classified Information

The Agency takes over classified information from public authorities that have ceased to exist and have no legal successor, or assigns another public authority for the storage and use of that information.

9.31. Central Register of Foreign Classified Information

The Agency establishes, maintains, and secures the Central Register of Foreign Classified Information and Documents.
A public authority that has received foreign classified information and documents in accordance with a special law or an international agreement concluded with a foreign state, international organization, or other international entity by the state, establishes, maintains, and secures a separate register of foreign classified information (Mijalkovski 2002, 128-130).
A report containing numerical indicators on the exchange of classified information with a foreign state or international organization is submitted by the public authority to the Agency at least once a year.
Notification and Reporting.
The Agency notifies the foreign state or international organization about the security of foreign classified information obtained through international exchange.
The Agency receives notifications from the foreign state or international organization about the security of classified information that the state has handed over in the international exchange.

9.32. Exchange of Information without a Concluded International Agreement

In extremely unfavorable political, economic, or defense-security circumstances for the state, and if necessary to protect interests, at the request of a public authority, the Agency may exchange classified information with a foreign state or international organization even without a previously concluded international agreement.

9.33. Supervision

Supervision over the implementation of this law and regulations enacted based on the law is conducted by the ministry responsible for justice (hereinafter: the Ministry).
In accordance with this law, during supervision, the Ministry:

1. Monitors the status in the field of classified information protection;
2. Prepares regulations necessary for implementing this law;
3. Provides opinions on draft regulations in the field of classified information protection;

4. Proposes to the Government the content, form, and method of maintaining records of classified information, as well as regulations governing the forms of security questionnaires, recommendations, certificates, and permits;
5. Orders measures to improve the protection of classified information;
6. Controls the application of criteria for marking security levels and performs other control tasks in accordance with the provisions of this law;
7. Files criminal complaints, requests for initiating misdemeanor proceedings, and proposes other proceedings for violations of the provisions of this law, in accordance with the law;
8. Cooperates with public authorities in implementing this law within its competence;
9. Performs other tasks provided by this law and regulations adopted based on this law.

The Minister responsible for justice submits an annual report on activities in the implementation and control of this law to the committee of the National Assembly competent for oversight and control in defense and security.

During supervision, the Ministry controls the implementation of measures for securing, using, exchanging, and other processing actions of classified information without prior notification of the public authority, authorized person, custodian, or user of the classified information. Tasks from paragraphs 1, 2, and 4 are carried out by authorized persons who have undergone special security checks.

Authorized persons conduct supervision by applying regulations on inspection supervision. Authorized persons have the right to official identification. Due to special working conditions, complexity, and nature of the job, authorized persons may receive a salary increase of up to 20% compared to the salary of civil servants and officials in the Ministry of Justice who perform supervisory duties over judicial bodies, in accordance with a Government act.

A detailed regulation on official identification and the work procedure of authorized persons is issued by the Minister responsible for justice.

10. PENAL PROVISIONS

10.1. Criminal Offense

Anyone who unauthorized discloses, hands over, or makes available data or documents entrusted to them or otherwise obtained, which constitute classified information marked as "INTERNAL" or "CONFIDENTIAL" under this law, shall be punished by imprisonment from three months to three years.

If the offense concerns data classified as "STRICTLY CONFIDENTIAL," the penalty shall be imprisonment from six months to five years.

If the offense concerns data classified as "STATE SECRET," the offender shall be punished by imprisonment from one to ten years.

If the offense is committed out of personal gain; or to publish or use classified information abroad, or during a state of war or emergency; the offender shall be punished by imprisonment from six months to five years.

If the offense is committed through negligence, the offender shall be punished by imprisonment, depending on the classification level, for a longer period according to legislation.

11. RELEVANT AREAS OF EMPIRICAL RESEARCH – RECOMMENDATIONS

By processing and analyzing the topic of this scientific paper, the following recommendations for organization and leadership in the security system can be drawn:

1. Reinstate and organize a separate Liaison Directorate and Criminal Police (KZ) structured along a clear chain of command, as it was before abolition.

2. Due to the nature of tasks and special personnel selection, restore authorizations and ranks according to job descriptions.
3. Attach the given service directly to the Police Director or to the new Service of the President of the Republic, the Service for the Protection of the Constitutional Order, the former RDB.
4. Reinstate legal procedures for secrecy and confidentiality classifications that clearly define levels and types.
5. Introduce, as a supplementary textbook, material clearly defining this issue to ensure a unified command chain, which has proven lacking among students and newly appointed managerial personnel.
6. Devote more attention and interpretation of secrecy to managerial staff, emphasizing the command line and its protection via communication systems in leadership and command, operational readiness of the service, and secrecy of its operatives in transmitting orders within the security system.
7. Pay more attention to the command chain in processing orders, which currently are handled over open networks, computers, and commercial electronic programs.

CONCLUSION

This scientific paper on organization and leadership in the security system presents elements of division and description of tasks both by work lines and territorial division. Every security organization, military or civilian, from the standpoint of preventive activity in intelligence or repressive action, must be structured according to the principles of jurisdiction and authority defined by the job description.
As shown above, to best understand the issue, an analysis was performed methodologically with empirical research and surveying citizens familiar with police organization and their opinions.
The further conclusion is that all activities and planning must be thoroughly organized, both the tasks themselves and the people who will lead and then execute the planned objectives.

REFERENCES

1. Aistrope Tim, and Roland Bleiker. 2018. "Conspiracy and foreign policy." *Security Dialogue* 49(3): 165-182.
2. Dentith, Matthew, and Martin Orr. 2018. “Secrecy and conspiracy” *Episteme* 15(4): 433 – 450.
3. Đorđević, Dejan. 2017. Mehanizmi prevencije za uspešno funkcionisanje sistema odbrane u vanrednim situacijama."*Vojno delo* 69(2): 219-249.
   DOI: 10.5937/vojdelo1702219D
   https://redun.educons.edu.rs/bitstream/handle/123456789/298/295.pdf?sequence=1&isAllowed=y
4. Horn, Eva. 2012. „Logics of Political Secrecy." *Theory, Culture & Society* 28(7-8):1-20. DOI: 10.1177/0263276411424583
   https://journals.sagepub.com/doi/abs/10.1177/0263276411424583
5. Humayun, Zafar. 2013. Human resource information systems: Information security concerns for organizations." *Human Resource Management Review* 23(1):105-113.
6. Mijalkovski, Milan. 2002. „Međunarodna baza podataka o teroristima.” *Vojno delo* 54(6): 127-145.
7. Olmsted, Kathryn. 2011. "Government secrecy and conspiracy theories." *Research in Social Problems and Public Policy* 19: 91-100.
8. Skolnick, Jerome. 1982. "Deception by the police." Criminal Justice Ethics 1(2):40-54.