
Warsaw, 19 August 2020

Opinion-Nr.: GEN-UKR/369/2019 [AIC]

OPINION ON THE DRAFT CONCEPT ON THE REFORM OF THE SECURITY SERVICE OF UKRAINE

UKRAINE

This Opinion has benefited from contributions made by Mr. Sami Faltas, Independent Expert on Security Sector Reform; Ms. Nazli Yildirim Schierkolk, Independent Expert on Security Sector Reform; the OSCE Conflict Prevention Centre and the Strategic Police Matters Unit, Transnational Threats Department, of the OSCE Secretariat.

Based on an unofficial English translation of the Draft Concept provided by the Security Service of Ukraine.



OSCE Office for Democratic Institutions and Human Rights

Ul. Miodowa 10, PL-00-251 Warsaw

Office: +48 22 520 06 00, Fax: +48 22 520 0605

www.legislationline.org

EXECUTIVE SUMMARY AND KEY RECOMMENDATIONS

ODIHR welcomes Ukraine's willingness to reform its Security Service (SSU), especially the stated objectives of SSU's demilitarization and of shifting its activities from law enforcement to counter-intelligence. However, the Draft Concept does not systematically demonstrate a human-rights based and gender- and diversity-sensitive approach to the reform. As they stand, several of its provisions can be applied in ways that may unduly restrict human rights and fundamental freedoms, including the rights to liberty and security, respect for private and family life, to a fair trial, to freedom of association as well as freedom of expression and access to information, especially if SSU's functions are not clearly regulated by law and subject to effective oversight.

It appears that the SSU will nevertheless retain law enforcement functions without clearly circumscribing their potential scope, nor providing strong safeguards. Such an amalgamation of functions is not in line with international standards and good practices, which call for a clear separation between intelligence and law enforcement functions, to avoid the risk of abuse of these powers. The Draft Concept should also explicitly provide that the legal framework pertaining to state secrets and classification of information, SSU's operational and search activities, including surveillance and covert measures, international co-operation and information exchange as well as the processing of personal data should be reviewed and revised, if necessary, to ensure compliance with international human rights standards. More detailed provisions or orientations relating to accountability and the mandate and powers of oversight mechanisms should also be included. In addition, gender and diversity should be mainstreamed throughout the Draft Concept to ensure that they are promoted internally as part of the working culture of the SSU, as well as externally when delivering security services.

Finally, it is essential that the Draft Concept be developed and adopted through a broad, inclusive and participatory process, which should subsequently guide the development of national security legislation and other programmes on the basis of such policy document.

More specifically, and in addition to what is stated above, ODIHR makes the following recommendations to further enhance the Draft Concept:

A. to revise the mandate of the SSU:

1. by removing from SSU's mandate the fight against organized crime, corruption, economic crimes and cybercrimes, or specifying that SSU is involved only when these crimes pose a clear and present danger to national security, and more generally ensure that SSU's mandate is systematically linked to the protection of national security, while ensuring that the constituting elements and threats to national security are strictly, clearly and exhaustively defined; [pars 48-52]
2. by ensuring that, throughout the Draft Concept, SSU's mandate is limited to intelligence/counter-intelligence activities and remove any law enforcement functions, such as criminal investigations, arrest and detention, from the

scope of the powers of the SSU and transfer them to the police and the prosecutorial/judicial authorities, as appropriate; or if deemed an absolute necessity and retained, strictly limit the scope and application of such law enforcement powers exclusively for combatting certain clearly defined national security criminal offences, when there is a reasonable suspicion that an individual has committed or is about to commit such offences or related preparatory/inchoate offences; specify that other law enforcement bodies shall not exercise law enforcement powers in relation to the same offences; and ensure that the exercise of these powers by the SSU is subject to the same legal safeguards and oversight that apply to other law enforcement agencies; [pars 54-59]

- B. to ensure that oversight not only focuses on the “*activities of the SSU*” but covers all aspects of the SSU’s functioning and work, while defining more clearly the scope, mandate and powers of the different control and oversight mechanisms and guaranteeing that they all have a right to access to all (classified) information relevant to their functions and necessary to discharge their responsibilities on the basis of procedure clearly defined by law; [pars 70-82]
- C. to stipulate the scope and extent of judicial oversight, both in term of *a priori* and *ex post facto* control, in particular the *ex-ante* authorisation of surveillance, the ongoing oversight of information collection measures and *ex-post* adjudication of cases; [par 81]
- D. to provide for strong policies and other safeguards, including proper and functioning reporting, complaints and disciplinary mechanisms to prohibit, prevent, detect and respond effectively to human rights violations, including sexual, gender-based and other types of abuse or harassment, intimidation, exploitation, violence or discrimination based on national or ethnic origin, colour, language, religion or belief, political or other opinion, gender, sexual orientation, gender identity, gender expression or any other ground, while ensuring the protection of whistle-blowers and complainants from retaliation by those accused of wrongdoing or by senior staff; [pars 92 and 99]
- E. to enhance the provisions concerning gender, diversity and non-discrimination, including by clearly stating the principle of non-discrimination as one of the key principles guiding the reform and the activities of SSU, and ensuring that gender and diversity are promoted internally as part of the working culture of the institution, as well as externally when delivering security services, and when budgeting and carrying out oversight; and [pars 85-95, 72 and 102]
- F. to explicitly recognize the human rights and fundamental freedoms of SSU personnel in the Draft Concept, while emphasizing that any restriction to their rights and freedoms should be strictly necessary and proportionate to ensure the political neutrality and impartiality of the public officials concerned and the proper performance of their duties. [pars 96-97]

As part of its mandate to assist OSCE participating States in implementing OSCE commitments, the OSCE/ODIHR reviews, upon request, draft and existing legislation to assess their compliance with international human rights standards and OSCE commitments and provides concrete recommendations for improvement.

TABLE OF CONTENT

I. INTRODUCTION	5
II. SCOPE OF REVIEW	5
III. ANALYSIS AND RECOMMENDATIONS	6
1. Relevant International Human Rights Standards and OSCE Human Dimension Commitments.....	7
2. General Comments	8
2.1. State Security and Human Security	8
2.2. Respect and Protection of Human Rights by the SSU.....	9
2.3. Terminology.....	10
2.4. Need of a Comprehensive Approach.....	10
3. Aim and Basic Principles of the Reform of the SSU	11
3.1. Rationale for Reforming the Security Service of Ukraine	11
3.2. Accountability	12
3.3. Transparency, Access to Information and Exception of State Secrets	13
3.4. Good Governance.....	14
3.5. Civil Direction and Status of the SSU	15
4. Mandate, Activities and Powers of the SSU.....	16
4.1. Mandate of the SSU	16
4.2. Operational and Search Activity	20
4.3. Data Collection and Processing	21
4.4. Information Exchange and Co-operation with Foreign Security Services	22
4.5. Other Comments.....	22
5. Control and Oversight over the Activities of the Security Service of Ukraine.....	23
5.1. Internal Control	24
5.2. Executive Control.....	25
5.3. Parliamentary Oversight.....	25
5.4. Parliament Commissioner for Human Rights.....	25
5.5. Judicial Accountability	26
5.6. Public Oversight.....	26
5.7. Prosecutor’s Office’s Supervision of Covert and Other Investigative and Search Actions	27
6. Gender and Diversity Considerations and Non-Discrimination.....	27
7. Human Resources Management and Financial and Logistical Support.....	30
7.1. Human Rights and Freedoms of SSU Personnel.....	30
7.2. Human Resources Management.....	32
7.3. Financial and Logistical Support	32
8. Final Comments on the Process of Preparing and Adopting the Draft Concept and Related Legislation.....	33
Annex: Draft Concept on the Reform of the Security Service of Ukraine	

I. INTRODUCTION

1. On 12 February 2020, the OSCE Project Co-ordinator in Ukraine forwarded to the OSCE Office for Democratic Institutions and Human Rights (ODIHR) a request from the Chair of the Security Service of Ukraine (SSU) to review the Draft Concept on the Reform of the Security Service of Ukraine (hereinafter “the Draft Concept”).
2. On 25 February 2020, ODIHR agreed to carry out a legal analysis of the Draft Concept to assess its compliance with OSCE human dimension commitments and international human rights and rule of law standards.
3. On 27 March 2020, ODIHR received a second request from the Chair of the Security Service of Ukraine to review the *Draft Law of Ukraine on Incorporating Amendments into the Law “On the Security Service of Ukraine”* (hereinafter “Draft Amendments”) that will be the subject of a separate legal analysis (hereinafter “ODIHR Opinion on the Draft Amendments”), which should be read together with this Opinion.¹
4. This Opinion was prepared in response to the above request. ODIHR conducted this assessment within its mandate to assist OSCE participating States in the implementation of key OSCE commitments in the human dimension.

II. SCOPE OF REVIEW

5. The scope of this Opinion covers only the Draft Concept submitted for review. Thus limited, the Opinion does not constitute a full and comprehensive review of the entire legal and institutional framework regulating the Security Service of Ukraine, though it should be read together with the *ODIHR Opinion on the Draft Amendments*.
6. The Opinion raises key issues and provides indications of areas of concern. In the interest of conciseness, the Opinion focuses more on those provisions that require improvements than on the positive aspects of the Draft Concept. The ensuing recommendations are based on international and regional standards, norms and practices as well as relevant OSCE human dimension commitments. The Opinion also highlights, as appropriate, good practices from other OSCE participating States in this field.
7. Moreover, in accordance with the *Convention on the Elimination of All Forms of Discrimination against Women*² (hereinafter “CEDAW”) and the *2004 OSCE Action Plan for the Promotion of Gender Equality*³ and commitments to mainstream a gender perspective into OSCE activities, programmes and projects, the analysis seeks to take into account the potentially different impact of the Draft Concept on women and men.
8. The Opinion is based on an unofficial English translation of the Draft Concept provided by the SSU, which is attached to this document as an Annex. Errors from translation may result. The Opinion is also available in Ukrainian. However, the English version remains the only official version of the Opinion.

¹ All legal reviews on draft and existing laws of Ukraine are available at: <<https://www.legislationline.org/odihr-documents/page/legal-reviews/country/52/Ukraine/show>>.

² *UN Convention on the Elimination of All Forms of Discrimination against Women* (hereinafter “CEDAW”), adopted by General Assembly resolution 34/180 on 18 December 1979. Ukraine deposited its instrument of ratification of this Convention on 12 March 1981.

³ See *OSCE Action Plan for the Promotion of Gender Equality*, adopted by Decision No. 14/04, MC.DEC/14/04 (2004), par 32.

9. In view of the above, ODIHR would like to stress that this review does not prevent ODIHR from formulating additional written or oral recommendations or comments on respective policy or related legislation regulating the SSU in the future.

III. ANALYSIS AND RECOMMENDATIONS

10. Human rights and fundamental freedoms are often curtailed for the presumed benefit of security. While human rights and security issues are sometimes conceptualised in an inverse relation to each other – i.e. in order to increase security one must reduce human rights, OSCE human dimension commitments and the UN approach underline that effective security measures and the protection of human rights are not conflicting but mutually reinforcing.⁴ As such, respect for human rights and fundamental freedoms for all, democracy and the rule of law is at the core of the OSCE’s comprehensive concept of security⁵ and should constitute the fundamental basis of any security sector reform, including reform of a security service.⁶ As noted by the OSCE Secretary General, “[e]xperience shows that an accountable, effective and inclusive security sector with full respect for human rights, including gender equality and the rule of law can effectively provide security to a State and its people, while at the same time promoting stability, trust and confidence in the OSCE area and beyond”.⁷
11. Threats to stability can arise through a security sector in which human rights and gender equality obligations are not properly fulfilled. The OSCE participating States have acknowledged⁸ the importance of the “human security” approach which places the rights and security needs of individuals at the heart of the security functions. This approach recognizes that the primary aim of security sector institutions is to adequately and effectively provide services to all individuals in the community, regardless of their national or ethnic origin, political or other opinion, sex, gender identity or sexual orientation, religion or belief or any other status.⁹ Security sector, including security services, is subject to the same standards of good governance as any other public sector, and is to provide security in an accountable and effective way, within a framework of democratic civilian control, rule of law and respect for human rights, including gender equality.¹⁰

⁴ ODIHR, [Background Paper on Addressing Transnational Threats and Challenges in the OSCE Region: the Human Dimension](#) (2012). See also UN General Assembly, 15 September 2005, [A/60/L.1](#), par 72; and UN Secretary-General, Kofi Annan, [Statement to the Security Council](#) on 18 January 2002.

⁵ OSCE, [Istanbul Charter for European Security](#) (1999), par 19.

⁶ See OSCE, [Charter on Preventing and Combating Terrorism](#), 10th Ministerial Council Meeting, Porto 2002, pars 5-7; and [OSCE Consolidated Framework for the Fight against Terrorism](#), adopted by Decision no. 1063 of the Permanent Council, at its 934th Plenary Meeting on 7 December 2012 (PC.DEC/1063). See also UN, [Global Counter-Terrorism Strategy and Plan of Action](#) (2006), Pillar IV; and [OSCE Ministerial Statement supporting the UN Global Counter-Terrorism Strategy \(MC.DOC/3/07\)](#), 30 November 2007). See also the [Joint Statement](#) of the UN High Commissioner for Human Rights, the Secretary General of the Council of Europe and ODIHR Director (29 November 2001).

⁷ OSCE Secretary General, [Report on the OSCE Approach to Security Sector Governance and Reform](#) (SSG/R) (2019), page 2.

⁸ OSCE, [Strategy to Address Threats to Security and Stability in the 21st Century](#), Maastricht, 2003.

⁹ See e.g., Geneva Centre for Security Sector Governance (DCAF), ODIHR and UN Women, [A Security Sector Governance Approach to Women, Peace and Security: Policy Brief](#) (2019), page 2; and ODIHR, [Background Paper on Addressing Transnational Threats and Challenges in the OSCE Region: the Human Dimension](#) (2012), page 2.

¹⁰ OSCE Secretary General, [Report on the OSCE Approach to Security Sector Governance and Reform](#) (SSG/R) (2019), page 2.

1. RELEVANT INTERNATIONAL HUMAN RIGHTS STANDARDS AND OSCE HUMAN DIMENSION COMMITMENTS

12. Key general international human rights applicable in Ukraine and which are relevant in the context of the security sector reform, and more specifically the reform of the SSU, are covered by the *International Covenant on Civil and Political Rights*¹¹ (ICCPR) and the *European Convention on Human Rights and Fundamental Freedoms*¹² (ECHR). In addition, Ukraine has also ratified, among others, the *UN Convention on the Elimination of All Forms of Discrimination against Women*¹³ (CEDAW), the *UN Convention on the Elimination of All Forms of Racial Discrimination*¹⁴ (CERD), the *UN Convention on the Rights of Persons with Disabilities*¹⁵ (CRPD), and the *UN Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment* (UNCAT).¹⁶ Concerning staffing-related issues within the SSU specifically, key international labour rights treaties ratified by Ukraine should also be considered.¹⁷
13. The [*UN Security Council Resolution 2151 \(2014\)*](#) on security sector reform also emphasizes the key role of security sector governance and reform (SSG/R) in contributing to peace and security. The [*UN Security Council Resolution 1325 “Women, Peace and Security”*](#) (WPS) (2000) and more broadly the *Women, Peace and Security Agenda*¹⁸ emphasize the importance of women’s full and equal participation in the security sector, and in decision-making on peace and security matters, while mandating the use of gender analysis for understanding conflict drivers, impacts, resolution and recovery options.¹⁹
14. At the Council of Europe level, in addition to the main human rights Conventions and Protocols, the [*Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*](#)²⁰ and the [*Convention on Access to Official Documents*](#)²¹ should also be taken into consideration when reforming the SSU, though the latter was only signed and not yet ratified by Ukraine.
15. At the OSCE level, participating States have recognized the need for a comprehensive, cross-dimensional response designed to address the multi-faceted causes of crises and conflicts in an effective and efficient manner.²² In addition to the CSCE and OSCE key

¹¹ *UN International Covenant on Civil and Political Rights* (ICCPR), adopted by the UN General Assembly by resolution 2200A (XXI) of 16 December 1966. Ukraine deposited its instrument of ratification of the ICCPR on 12 November 1973.

¹² Council of Europe (Coe), *Convention for the Protection of Human Rights and Fundamental Freedoms*, entered into force on 3 September 1953. Ukraine deposited its instrument of ratification of the ECHR on 11 September 1997.

¹³ *UN Convention on the Elimination of All Forms of Discrimination against Women* (CEDAW), adopted by the UN General Assembly by resolution 34/180 of 18 December 1979. Ukraine deposited its instrument of ratification of the CEDAW on 12 March 1981 and of its Optional Protocol on 26 September 2003.

¹⁴ *UN International Convention on the Elimination of All Forms of Racial Discrimination* (CERD), adopted by the UN General Assembly by resolution 2106 (XX) of 21 December 1965. Ukraine deposited its instrument of ratification of this Convention on 7 March 1969.

¹⁵ *UN Convention on the Rights of Persons with Disabilities* (CRPD), adopted by the UN General Assembly by resolution A/RES/61/106 of 13 December 2006. Ukraine ratified this Convention and its Optional Protocol on 4 February 2010.

¹⁶ *UN Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment* (UNCAT), adopted by the UN General Assembly by resolution A/RES/39/46 of 10 December 1984. The UNCAT was ratified by Ukraine on 24 February 1987 and its Optional Protocol on 19 September 2006.

¹⁷ See the conventions of the International Labour Organization (ILO) ratified by Ukraine (<https://www.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:11200:0::NO::P11200_COUNTRY_ID:102867>).

¹⁸ As of 5 May 2020, the UN Security Council has adopted ten resolutions on “Women, Peace and Security”, which together make up the Women, Peace and Security Agenda: [1325 \(2000\)](#); 1820 (2009); 1888 (2009); 1889 (2010); 1960 (2011); 2106 (2013); 2122 (2013); 2242 (2015), 2467 (2019), and 2493 (2019).

¹⁹ See e.g., UN Security Council, [Resolution 2122 on Women, Peace and Security](#) (2013), pars 7 and 14, which “recognizes the continuing need to increase women’s participation in maintenance of peace and security. stresses the need for continued efforts to address obstacles in women’s access to justice in conflict and post-conflict settings, including through gender-responsive legal, judicial and security sector reform and other mechanisms; [...] and to ensure women’s full and meaningful participation in efforts to combat and eradicate the illicit transfer and misuse of small arms and light weapons”; and [Resolution 2242 \(2015\)](#), especially pars 11 and 15, which emphasizes the need for the integration of gender within counterterrorism and efforts to counter violent extremism, in particular through integrating a gender perspective into assessments and reports.

²⁰ Council of Europe, [Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data](#) (CETS No. 108), 28 January 1981, ratified by Ukraine on 30 September 2010 and which entered into force on 1 January 2011.

²¹ Council of Europe, [Convention on Access to Official Documents](#) (CETS No. 205), 18 June 2009, signed by Ukraine on 12 April 2018, but has not yet been ratified.

²² OSCE, [Ministerial Council Decision No. 3/11](#) (MC.DEC/3/11) on Elements of the Conflict Cycle.

commitments,²³ the 1994 [OSCE Code of Conduct on Politico-Military Aspects of Security](#) is also an essential document in this regard and sets out basic norms for the democratic control of armed and security forces, as well as ensuring human rights and fundamental freedoms for military, paramilitary and security forces personnel.

16. The ensuing recommendations will also make reference, as appropriate, to other specialized documents of a non-binding nature, which have been endorsed in various international or regional fora and may prove useful as they contain a higher level of details.²⁴ In particular, the new [2019 DCAF-ODIHR-UN Women Gender and Security Toolkit](#),²⁵ especially *Tool no. 14 on Intelligence and Gender*, provides practice-based policy and programmatic guidance to integrate a gender perspective and advance gender equality in security and justice policy, programming and reform, including in intelligence services but also with regard to the parliamentary oversight of the security sector.

2. GENERAL COMMENTS

2.1. State Security and Human Security

17. While several provisions of the Draft Concept do refer to the respect for and/or protection of human (and civil) rights and freedoms (Sections 1.1, 1.4 second indent, 2.1, 2.2, 3.1, 4, 8.1 and 9), it appears that the Draft Concept primarily focuses on the protection of “*state security*” or “*national security*” of Ukraine (see Sections 1.1, 1.3, 1.4, 1.5, 2.1, 3.1, 3.2, 4, 5.2 and 9), without referring to the security of all individuals (“*human security*”).
18. Traditionally, it was common for governments and their security agencies to exclusively or primarily focus on the security of the state. More recently, governments have increasingly widened the scope of their security policy to take all threats into account that could confront all individuals in their country, thus considering the rights and security and justice needs, concerns and expectations of all individuals, women, men, girls, boys and marginalized persons or groups across different parts of the community.²⁶ The ultimate aim is to provide better, more nuanced and effective responses to these needs.²⁷ It is key that such security needs be defined in an inclusive, gender-responsive manner,²⁸ ensuring

²³ See especially, CSCE/OSCE, [1975 Helsinki Final Act 1975](#) (Questions Relating to Security in Europe: 1.(a) Declaration on Principles Guiding Relations between Participating States, Principle VII); [1990 Copenhagen Document](#), Preamble and pars 1 and 41; [1992 Helsinki Document](#) (Summit Declaration), par 21; [1994 Budapest Document](#) (Summit Declaration), par 14; [2003 Maastricht Document](#) (OSCE Strategy to Address Threats to Security and Stability in the Twenty-First Century; Threats to security and stability in the twenty-first century), pars 4 and 9; [2010 Astana Commemorative Declaration: Towards a Security Community](#), pars 2 and 6.

²⁴ These include e.g.: the [Compilation of Good Practices on Legal and Institutional Frameworks and Measures that Ensure Respect for Human Rights by Intelligence Agencies while Countering Terrorism, including on their Oversight](#) (2010), developed by the UN Special Rapporteur on the protection and promotion of human rights while countering terrorism, as mandated by the UN Human Rights Council (hereinafter “UN SRCT Compilation”); CoE Commissioner for Human Rights, [Issue Paper on Democratic and Effective Oversight of National Security Services](#), (2015); CoE Parliamentary Assembly (PACE), [Recommendation 1402 \(1999\) on the Control of Internal Security Services in Council of Europe Member States](#) (1999); [Recommendation 1713 \(2005\) on Democratic Oversight of the Security Sector in the Member States](#) (2005); [Resolution 1838 \(2011\) on Abuse of State Secrecy and National Security: Obstacles to Parliamentary and Judicial Scrutiny of Human Rights Violations](#) and [Resolution 2060 on Improving the Protection of Whistleblowers](#) (2015); CoE, European Commission for Democracy through Law (Venice Commission), [Report on the Democratic Oversight of the Security Services](#), CDL-AD(2015)010; [Report on the Democratic Oversight of Signals Intelligence Agencies](#), CDL-AD(2015)011; [2015 Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Agencies](#), CDL-AD(2015)006; and 2007 [Report on the Democratic Oversight of the Security Services](#), CDL-AD(2007)016; NATO Parliamentary Assembly-DCAF, Yildirim Schierkolk, Nazli, [Parliamentary Access to Classified Information](#) (2018); European Parliament, Committee on Civil Liberties, Justice and Home Affairs, [Study on the Parliamentary Oversight of Security and Intelligence Agencies in the European Union](#) (2011); European Union Agency for Fundamental Rights (FRA), [Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU - Mapping Member States' legal frameworks](#) (2015); the [Global Principles on National Security and the Right to Information](#) (Tshwane Principles), developed and adopted on 12 June 2013 by a large assembly of experts from international organizations, civil society, academia and national security practitioners.

²⁵ DCAF – OSCE/ODIHR and UN Women, [Gender and Security Toolkit](#) (2019).

²⁶ See e.g., DCAF-OSCE/ODIHR-UN Women, [Policy Brief on Security Sector Governance Approach to Women, Peace and Security](#) (2019); UN Secretary-General, [Report on Securing States and Societies: Strengthening the United Nations Comprehensive Support to Security Sector Reform](#), 13 August 2013, A/67/970–S/2013/480, par 61 (a); and OECD DAC, [Handbook on Security Sector Reform](#) (2007).

²⁷ *Op. cit.* footnote 25, page 5 (2019 DCAF-OSCE/ODIHR-UN Women Tool no. 1 on SSG/SSR and Gender).

²⁸ *ibid.* (2019 DCAF-OSCE/ODIHR-UN Women Tool no. 1 on SSG/SSR and Gender).

that communities and individuals participate in articulating their own needs. This is likely to increase the local acceptance of justice and security actors, as well as giving such actors important insights as to how to improve in fulfilling their tasks.²⁹ The concept of good SSG is nowadays understood in a broader manner, using the security needs of humans as a starting point – an approach enshrined in the concept of “*human security*” adopted by [UN General Assembly Resolution 66/290](#) in 2012 and endorsed by OSCE participating States (see par 11 *supra*). Many States have enshrined this principle in their security policies and national laws, requiring their intelligence/security services to fulfil their mandates in a manner that serves the interests of the State and society as a whole.³⁰

19. At the same time, the Law on National Security of Ukraine (2018) states in Article 3 par 1 that “[t]he state policy in the fields of national security and defence is aimed at protection of: human and citizen - their lives and dignity, constitutional rights and freedoms, safe living conditions; society - its democratic values, prosperity and conditions for sustainable development; the state - its constitutional order, sovereignty, territorial integrity and inviolability; territory, the environment - from emergencies”. Similarly, while Ukraine’s current National Security Strategy still focuses on the security of the state, it is understood that the new upcoming strategy reportedly called “*Security of a Person – Security of a Country*” will be more person-oriented.³¹ These latest developments suggest that “*human security*” is now the focus of Ukraine’s new national security policy, which is a welcome development.
20. In light of the above, it is recommended that **the Draft Concept also refers to both state and human security whenever appropriate**, all the more since according to Section 1.1 of the Draft Concept, it is based on Ukraine’s National Security Strategy, among others. At the same time, more than a mere change of terminology, such an approach also requires mainstreaming the security needs of all individuals, taking into account their diversity, throughout policies and legislation, promoting human security more generally, while providing strong human rights safeguards throughout the Draft Concept (see Sub-Sections 2.2 and 6 *infra*). Furthermore, the process of devising policy and legislation in the sphere of security should also be more inclusive and participatory, and include human security considerations (see Sub-Section 8 *infra*).

2.2. Respect and Protection of Human Rights by the SSU

21. The first paragraph of Section 1.1 refers to a number of legal documents on which the Draft Concept should be based, which includes a reference to several legal and policy documents of Ukraine as well as the Association Agreement between Ukraine and the EU. Several subsequent provisions of the Draft Concept make an explicit reference to respect for and/or protection of human (and civil) rights and freedoms (see Sections 1.1, 1.4 second indent, 2.1, 2.2, 3.1, 4, 8.1 and 9 of the Draft Concept) and to international human rights law (Sections 1.3, 2.2 and 9). While it is good practice to do so,³² **it would be advisable to expressly state at the outset in Section 1.1 that the reform of the SSU is also based on binding international law and human rights obligations.**
22. At the same time, such a statement referring to international standards by itself is unlikely to be effective in practice if the whole Draft Concept does not demonstrate a human-rights based and gender- and diversity-sensitive approach to the reform. As they stand, several of its provisions can be applied in ways that may unduly restrict human rights and fundamental freedoms, including the rights to liberty and security, respect for private and

²⁹ *ibid.* page 27 (2019 DCAF-OSCE/ODIHR-UN Women Tool no. 1 on SSG/SSR and Gender).

³⁰ *Op. cit.* footnote 24, par 18 (2010 UN SRCT Compilation).

³¹ See <<https://www.president.gov.ua/en/news/rbbo-rozglvanula-proekt-strategiyi-nacionalnoyi-bezpeki-ukra-59321>>.

³² *Op. cit.* footnote 24, par 12 (2010 UN SRCT Compilation).

family life, to a fair trial, to freedom of association as well as freedom of expression and access to information (e.g., Sub-Sections 2.2., 3.1, 5.2, 5.3 of the Draft Concept), especially if SSU's functions are not clearly regulated by law and subject to effective oversight. Generally, security services by their very nature and the powers conferred to them have the potential to impinge on individual rights and fundamental freedoms, which may be legitimate only in limited circumstances, where prescribed by law and strictly necessary and proportionate, and subject to external scrutiny.

23. In case the SSU is mandated to carry out activities abroad, such actions should be implemented in compliance with the Constitution and international human rights standards.³³ Indeed, the case law of the ECtHR and the UN Human Rights Committee clarifies that human rights obligations under the relevant treaties can extend to activities conducted wholly extraterritorially.³⁴ If relevant, **this should be explicitly stated in the Draft concept.**

2.3. Terminology

24. Certain provisions of the Draft Concept refer to “*a person and a citizen*” (Section 1.1) while others exclusively refer to “*every citizen*” (Section 1.4, 2nd indent) or to the “*Ukrainian people*” (Section 4). Throughout the Draft Concept, it would be advisable to refrain from referring exclusively to “*citizens*” or “*Ukrainian people*” since they form a subset of all persons under the jurisdiction of the State,³⁵ which also include non-citizens, such as foreign nationals, migrants, asylum-seekers, refugees and stateless persons.
25. The Draft Concept also mentions the rights and freedoms of “*citizens*”. It is worth emphasizing that guarantees of fundamental rights and freedoms should apply to everyone, and not just to citizens,³⁶ except for certain specific rights that may apply only to citizens, e.g., the right to vote and to be elected. Especially, as per the [Compilation of Good Practices on Legal and Institutional Frameworks and Measures that Ensure Respect for Human Rights by Intelligence Agencies while Countering Terrorism, including on their Oversight \(2010\)](#) developed by the UN Special Rapporteur on the protection and promotion of human rights while countering terrorism (hereinafter “UN SRCT Compilation”), intelligence services shall carry out their work in a manner that contributes to the promotion and protection of the human rights and fundamental freedoms of all individuals under the jurisdiction of the State.³⁷
26. In light of the foregoing, the terms “*citizens*” and “*Ukrainian people*” where relevant should **be replaced or supplemented by the wording “all individuals” or “everyone” throughout the Draft Concept, as appropriate.**

2.4. Need of a Comprehensive Approach

27. Section 1.5 of the Draft Concept mentions a “*comprehensive process of reforming other components of the security and defense sector of Ukraine to create an effective system of*

³³ *ibid.* Practice 5 (2010 UN SRCT Compilation).

³⁴ See e.g., ECtHR, [Ilaşcu and Others v. Moldova and Russia](#) [GC] (Application no. 48787/99, judgment of 8 July 2004); [Öcalan v. Turkey](#) [GC] (Application no. 46221/99, judgment of 12 May 2005); [Al-Saadoon & Mufdhi v. the United Kingdom](#) (Application no. 61498/08, judgment of 2 March 2010). See also UN Human Rights Committee (CCPR), [General Comment no. 36 on Article 6 of the ICCPR](#) (30 October 2018), par 63; and 2014 [Concluding Observations on the Fourth Report on the United States of America](#) (CCPR/C/USA/CO/4), par 22 (a), which states that the State should “[t]ake all necessary measures to ensure that its surveillance activities, both within and outside the United States, conform to its obligations under the Covenant, including article 17; in particular, measures should be taken to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity, regardless of the nationality or location of the individuals whose communications are under direct surveillance”.

³⁵ See e.g., Venice Commission, [Report on the Democratic oversight of Signals Intelligence Agencies](#), CDL-AD(2015)011, par 72.

³⁶ See e.g., ODIHR, [Comments on the Draft Constitution of Turkmenistan](#) (2016), par 132. See also e.g., Venice Commission, [Opinion on the Draft Law on the Review of the Constitution of Romania](#), CDL-AD(2014)010, 24 March 2014, par 49; [Opinion on the Constitution of Bulgaria](#), CDL-AD(2008)009, 31 March 2008, pars 55-57.

³⁷ *Op. cit.* footnote 24, Practice 11 (2010 UN SRCT Compilation).

countering threats to national security of Ukraine". It is generally acknowledged that the effectiveness of a security sector reform requires a more comprehensive approach to SSG/R also calling for links to be established between different reform processes that are mutually reinforcing (police, justice, intelligence, etc.), instead of these processes being dealt with individually.³⁸ A recent mapping study concerning SSR in Ukraine specifically recommend to ensure greater linkages between the SSU and justice reform.³⁹

28. Therefore, **it is recommended that the linkages with the reform of other components of the security sector (particularly the police and justice) be emphasized more prominently and explained in the Draft Concept.** It is also key that the relations and coordination with law enforcement agencies and the judiciary, including the fact that SSU's activities shall be subject to judicial control,⁴⁰ be clearly regulated, not to leave space to subjective interpretation and avoid abusive practices in such very sensitive areas. In that respect, it is recommended that **the coordination and interaction of the SSU mentioned in Section 2.2 not be limited to the security and defence sector, but that this provision also expressly mentions the police and the justice sector.**

3. AIM AND BASIC PRINCIPLES OF THE REFORM OF THE SSU

3.1. Rationale for Reforming the Security Service of Ukraine

29. Section 1.4 of the Draft Concept lists the main reasons for reforming the SSU. While the list is clearly developed based on national priorities, there are several considerations that could be reflected to increase compliance with international standards and guidance.
30. Section 1.4, 1st indent, refers to "*incitement of separatism in certain regions of Ukraine*". Such a wording should not be used as an excuse to gather intelligence on persons or organizations which may simply express opinions, however shocking and unacceptable certain views or words used may appear to the authorities and/or the population, when there is no real foreseeable risk of violent action or of incitement to violence or any other form of rejection of democratic principles. As expressly stated by the ECtHR, "*the fact that a group of persons calls for autonomy or even requests secession of part of the country's territory – thus demanding fundamental constitutional and territorial changes [...] does not automatically amount to a threat to the country's territorial integrity and national security*".⁴¹ Accordingly, **the wording should be more clearly defined and strictly circumscribed, so as to prevent abuses. At a minimum, there should be a clear reference to an actual (objective) risk of violent action or of incitement to violence or any other form of rejection of democratic principles.** Otherwise, this risks creating a chilling effect on the exercise of freedom of association and expression, and could stifle debate on contentious issues.
31. As to the organization structure of the SSU (Section 1.4, 5th indent), **it may be advisable to also include the principle of "professionalism" in the context of optimizing SSU's organizational structure and staffing.** As recommended at the international level, this entails developing "*an institutional culture of professionalism based on respect for the rule of law and human rights' through establishing ethical standards and codes of conduct, as*

³⁸ See e.g., OSCE Secretary General, *Report on the OSCE Approach to Security Sector Governance and Reform (SSG/R)* (2019), pages 5 and 11; and *op. cit.* footnote 26, par 61(e) (2013 UN Secretary-General's *Report on Securing States and Societies*).

³⁹ See DCAF, *Supporting Ukraine's Security Sector Reform – Mapping Security Sector Assistance Programmes* (2018), page 193.

⁴⁰ *Op. cit.* footnote 24, par C.3 (1999 PACE Recommendation 1402).

⁴¹ See ECtHR, *Stankov and the United Macedonian Organisation Ilinden v. Bulgaria* (Applications nos. 29221/95 and 29225/95, judgment of 2 October 2001), par 97.

well as developing a rigorous and continuous training of staff on national and international standards”.⁴²

32. Section 2.1 outlines the main objectives of the reform. In view of the foregoing, **Section 2.1 could further specify that the key characteristics of the SSU should not only be its effectiveness, dynamism and flexibility but also its inclusiveness.** Moreover, the provision should go beyond merely referring to “*well-trained*” personnel to specify that **they should uphold the highest professional and ethical standards.** It could also **further state that the tasks, functions and directions of the SSU shall comply with human rights and freedoms, and that the SSU is equipped to exercise its functions within the mandate prescribed by laws, subject to accountability and oversight mechanisms.** As demilitarization of the SSU is also a priority, this could be further emphasized in Section 2.1 of the Draft Concept (see also Sub-Section 3.5 *infra*).

3.2. Accountability

33. Section 2.2, last indent, of the Draft Concept refers to “*democratic civilian control*”, as does Section 1.4, last indent. At the same time, it is not clear what exactly this refers to, especially whether this implies internal control by civilian authorities and/or the executive and/or mechanisms of oversight by the parliament, judiciary, other independent bodies, the public etc. It would be advisable **to specify in Section 2.2, last indent, that democratic and civilian oversight of the SSU includes internal and executive control, as well as oversight by parliamentary, judicial and specialized public oversight mechanisms** (see also Sub-Section 5 *infra* on control and oversight over the SSU).
34. **The Section should also expressly refer to accountability, as this constitutes a key principle that should guide any reform of the security sector, including of security services.**⁴³ It would also be important to further explain what the principle of accountability would entail. Indeed, the obligations to investigate human rights violations or other illegal acts, reveal the truth, and ensure accountability, especially in anti-terrorist operations, has been noted, and is reflected in some detail at the international level, for instance in the reports of the UN Special Rapporteur on counter-terrorism.⁴⁴ This principle helps ensuring that those responsible are brought to justice, promoting accountability and preventing impunity, avoiding denial of justice and drawing necessary lessons for revising practices and policies with a view to avoiding repeated violations.⁴⁵
35. In that respect, the principle of “*individual responsibility*” together with States’ obligation to bring perpetrators to justice are firmly enshrined in relevant legal instruments concerning the most serious human rights violations, such as the *UNCAT* (Articles 2, 4 and 6) and the *International Convention for the Protection of All Persons from Enforced Disappearance* (Articles 6 and 23).⁴⁶ Based on those principles, the UN SRCT Compilation recommends that “[n]ational laws provide for criminal, civil or other sanctions against any member, or individual acting on behalf of an intelligence service, who violates or orders an action that would violate national law or international human rights law. These laws also establish procedures to hold individuals to account for such violations”.⁴⁷ The CoE European Commission for Democracy through Law (Venice

⁴² *Op. cit.* footnote 24, Practice 19 (2010 UN SRCT Compilation).

⁴³ *Op. cit.* footnote 24, Section V (2015 Venice Commission’s [Report on the Democratic Oversight of the Security Services](#)).

⁴⁴ See e.g., UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (hereafter “UN Special Rapporteur on counter-terrorism”), [Framework Principles for Securing the Accountability of Public Officials for Gross or Systematic Human Rights Violations Committed in the Course of States-sanctioned Counter-terrorism Initiatives](#) (2013) A/HRC/22/52.

⁴⁵ CCPR, [General Comment no. 36 on Article 6 of the ICCPR](#) (30 October 2018), par 27.

⁴⁶ See also Article 33 of the Rome Statute of the International Criminal Court, which was signed by Ukraine on 20 January 2000, though has yet to be ratified.

⁴⁷ *Op. cit.* footnote 24, Practice 16 (2010 UN SRCT Compilation).

Commission) also highlights the need for security services to set up internal procedures to establish and trace individual responsibility for violating laws or other abuses of power.⁴⁸ Additionally, accountability also implies that superior officials shall be held responsible for the actions of persons under their command if the superior official knew or should have known of abuses but failed to take concrete action; also, public officials who refuse unlawful superior orders shall be given immunity and those who commit abuses shall not be excused on the grounds that they were following superior orders.⁴⁹ **These aspects should be reflected in Section 2.2 when referring to accountability.** Finally, Section 4, 5th indent, states that the SSU is “*responsible to the Ukrainian people*”. If the aim is to underline accountability, **the sentence could be revised to reflect a broader understanding of accountability towards the executive, the judiciary, and the legislative branches of Ukraine as well as to the public** (see Sub-Section 5 *infra*).

3.3. Transparency, Access to Information and Exception of State Secrets

36. Sections 1.4 and 2.2 of the Draft Concept refer to the “*optimal balance between transparency and conspiracy [understood by ODIHR as secrecy]*”. Such a statement is rather vague and fails to acknowledge that access to information and openness, which are necessary conditions for democratic governance and protection of human rights, should be the starting point, and secrecy the exception.⁵⁰ Transparency is key to enhance public trust in the SSU and should be a key principle guiding the reform of the SSU, in line with good practices of SSG.⁵¹ Except when certain limitations to access to information are prescribed by law, necessary and proportionate to prevent specific, identifiable harm to legitimate interests,⁵² information should be available and accessible, especially to those who will be affected by SSU’s decisions and their implementation, as well as by those in charge of the oversight of the SSU to ensure accountability. **It is recommended to rephrase this wording in the Draft Concept to put emphasis on openness, transparency and accessibility, subject to strictly necessary and proportionate exceptions to protect national security.**
37. In particular, as recommended at the international level, there should be transparency about certain aspects of the functioning and activities of intelligence/security services, including the structures and powers of such services, as defined in law; information for evaluating and controlling the use of public funds; the existence and terms of bilateral and multilateral agreements between them and relevant bodies of other countries; and the overall legal framework for the use of surveillance of all kinds.⁵³ The *ODIHR Opinion on the Draft Amendments* relating to the SSU elaborates further the recommendations to enhance the human rights compliance of the legal framework relating to access to information and state secrets.
38. At the same time, **the Draft Concept should specify that the legal framework on access to information and the protection of state and other secrets and classification of information in Ukraine should be reviewed to ensure compliance with international law and standards, especially the 2008 Council of Europe Convention on Access to**

⁴⁸ *Op. cit.* footnote 24, pars 131, 132 and 181 (2007 Venice Commission’s [Report on the Democratic Oversight of the Security Services](#)).

⁴⁹ See e.g., Article 2 of UNCAT and par 26 of the General Comment No. 2 of the UNCAT Committee; Articles 6 and 23 of the International Convention for the Protection of All Persons from Enforced Disappearance. See also e.g., the [Updated Set of Principles for the Protection and Promotion of Human Rights through Action to Combat Impunity](#), recommended by the United Nations Commission on Human Rights Resolution no. 81/2005 of 21 April 2005, E/CN.4/2005/102/Add.1, Principle 27; the [UN Basic Principles on the Use of Force and Firearms by Law Enforcement Officials](#) (1990), Principles 24 to 26; and [UN Code of Conduct for Law Enforcement Officials](#) (1979), Article 5.

⁵⁰ See e.g., DCAF, [Overseeing Intelligence Services: A Toolkit](#) (2012), page 53.

⁵¹ *Op. cit.* footnote 25, page 13 (2019 DCAF-OSCE/ODIHR-UN Women Tool no. 1 on SSG/SSR and Gender).

⁵² *Op. cit.* footnote 24, Principles 1 and 3 (Tshwane Principles).

⁵³ *ibid.* Principle 10 (Tshwane Principles).

Official Documents.⁵⁴ This should aim to **ensure that it is not overbroad or vague, and that the rights to freedom of expression and access to information of journalists, civil society representatives, media outlets and private individuals are not unduly restricted on this basis.**

39. Other provisions of the Draft Concept refer to the development and implementation of an effective communication strategy to inform the public about SSU's activities (Section 3.1, 22nd indent, and Section 3.2). In that respect, it is good practice to publish figures regarding the operation of the intelligence service, such as those regarding the notification and non-notification of the target of surveillance (when this no longer jeopardize confidential methods), the number of individuals and the number of communications subject to surveillance each year and other aggregate statistics.⁵⁵ **These aspects could be reflected in the Draft Concept or in relevant legislation. It is also key that the Draft Concept makes it clear that the public should also be properly informed about the SSU's structures and powers in a clear and understandable manner, and about applicable laws and regulations,⁵⁶ including by providing clear information about the circumstances and conditions in which a person can be subject to surveillance.**

3.4. Good Governance

40. It is welcome that Section 1.4, 5th indent, of the Draft Concept refers to the principles of good governance of the SSU, as also stated in Section 2.2, 5th indent. Indeed, the principle of good Security Sector Governance is specifically endorsed by the OSCE Secretary General and in UN Secretary-General's reports on security sector reform.⁵⁷
41. At the same time, some of the other principles listed under Section 2.2 such as rule of law, legality, transparency and democratic civilian control (accountability) are generally considered to be key components of good governance and are therefore somewhat redundant if kept separate from the concept of good governance. It would be important to **specify more clearly what is meant by "good governance" in the context of the reform of the SSU, by referring to accountability, transparency, rule of law, participation, responsiveness, effectiveness and efficiency, and specify what these terms entail.⁵⁸ Gender equality and diversity are also central elements of the principles of good SSG, and should be reflected.⁵⁹**

⁵⁴ Council of Europe, [Convention on Access to Official Documents](#) (CETS 205), 2008, signed by Ukraine on 12 April 2018, though not yet ratified.

⁵⁵ See *op. cit.* footnote 24, par 137 (2015 Venice Commission's [Report on the Democratic Oversight of the Security Services](#)); and [PACE, Resolution 2045\(2015\) on Mass surveillance](#), 21 April 2015, par 13. See also *op. cit.* footnote 24, Principle 10.E (2) (2013 Tshwane Principles).

⁵⁶ *Op. cit.* footnote 24, Principle 10 (2013 Tshwane Principles), including laws and regulations applicable to the SSU and its oversight bodies and internal accountability mechanisms, information needed for evaluating and controlling the expenditure of public funds, and the overall legal framework concerning surveillance of all kinds, as well as the procedures to be followed for authorizing surveillance, selecting targets of surveillance, and using, sharing, storing, and destroying intercepted material, should be accessible to the public, etc.

⁵⁷ See OSCE Secretary General, [Report on the OSCE Approach to Security Sector Governance and Reform](#) (SSG/R) (2019), pages 1-2; and UN Secretary-General, [Report on Securing Peace and Development: The Role of the United Nations in Supporting Security Sector Reform](#), 23 January 2008, A/62/659 –S/2008/39; and [Report on Securing States and Societies: Strengthening the United Nations Comprehensive Support to Security Sector Reform](#), 13 August 2013, A/67/970–S/2013/480.

⁵⁸ See e.g., *op. cit.* footnote 25, pages 13-14 (2019 DCAF-OSCE/ODIHR-UN Women Tool no. 1 on SSG/SSR and Gender), which refer to "**Accountability**: the security sector must be held accountable for meeting the diverse needs of all sectors of the population; **Transparency**: information is freely available and accessible to those who will be affected by decisions and their implementation; **Rule of law**: all persons and institutions, including the state, are subject to laws that are known publicly, enforced impartially and consistent with international and national human rights norms and standards; **Participation**: all persons of all backgrounds have the opportunity to participate in decision-making and service provision on a free, equitable and inclusive basis, either directly or through legitimate representative institutions; **Responsiveness**: institutions are sensitive to the different security needs of all parts of the population, and perform their missions in the spirit of a culture of service and without discrimination; **Effectiveness**: institutions fulfil their respective roles, responsibilities and missions to a high professional standard according to the diverse needs of all parts of the population; and **Efficiency**: institutions make the best possible use of public resources in fulfilling their respective roles, responsibilities and missions.

⁵⁹ See e.g., OSCE Secretary General, [Report on the OSCE Approach to Security Sector Governance and Reform](#) (SSG/R) (2019), page 5.

3.5. Civil Direction and Status of the SSU

42. It is overall welcome that Section 3.1, 10th indent, of the Draft Concept announces a demilitarization of the SSU and Section 3.2 provides some details on how this will be done, though nothing specific is said concerning civil direction and control. In the [OSCE Moscow Document](#) (1991), OSCE participating States committed to ensure that their security agencies, including intelligence services “*are subject to the effective direction and control of the appropriate civil authorities*”. In other words, security agencies should be directed by civil authorities with a constitutional mandate and democratic legitimacy. **It is important that this principle is clearly stated in the Draft Concept.**
43. Section 2.2 of the Draft Concept refers to “*non-partisanship, political neutrality and independence*” of the SSU as one of the key principles of the reform. Section 4 further states that the SSU is “*politically and operationally independent*”. This is overall welcome and in line with international good practice that recommends that national law should prohibit intelligence services from engaging in any political activities or from acting to promote or protect the interests of any particular political, religious, linguistic, ethnic, social or economic group.⁶⁰ However, apart from provisions concerning the Head of the SSU (Section 3.1, 11th indent), nothing is said as to how such neutrality and independence would be ensured.
44. The Head of the SSU is appointed and dismissed by the Verkhovna Rada of Ukraine upon the recommendation of the President of Ukraine. As per Article 19 of the Law on National Security of Ukraine (2018), the SSU is subordinated to the President and under the control of the Verkhovna Rada. After the reforms announced in the Draft Concept, the SSU Head’s term of office will be fixed by law in such a way that it does not coincide with the President’s term of office. The law will also limit grounds for dismissal of the SSU Head (Section 3.1, 11th indent, of the Draft Concept). This arrangement will potentially limit the risk of the SSU being used for inappropriate political purposes by the President or Parliament, who will be jointly responsible for the SSU. It is noted that there is no Ukrainian minister specifically responsible for the SSU and giving it detailed political guidance, the way ministers of defence direct the military.⁶¹ The Parliamentary Assembly of the Council of Europe explicitly recommends having a single minister to control and supervise security services.⁶² **The drafters should consider such an option.**
45. **Safeguards against political interference can also be further enhanced by introducing legally determined procedures for appointing the Head of the SSU.** While there is no single prescriptive international standard stipulating how heads of security services should be appointed, there is a number of country good practices suggesting that nomination or appointment procedures should not be left to the sole discretion of the executive, should be based on publicly available laws and clear and apolitical criteria, and should include some form of consultation with the Parliament ensuring broad political backing or other scrutiny from outside the executive, while ensuring that the process is transparent and merit-based.⁶³ **It is recommended that the Draft Concept specifies that the**

⁶⁰ *Op. cit.* footnote 24, Practice 12 (2010 UN SRCT Compilation). See also [1994 OSCE Code of Conduct on Politico-Military Aspects of Security](#), par 23; and *op. cit.* footnote 24, par 15d (2005 PACE Resolution 1713), which states that “[u]nder no circumstances should the intelligence services be politicized as they must be able to report to policy makers in an objective, impartial and professional manner”.

⁶¹ In Ukraine, the Chief of Defence Staff also reports to the President. (Article 16 par 3 of the 2018 Law on National Security of Ukraine).

⁶² *Op. cit.* footnote 24, par C.1 (1999 PACE Recommendation 1402), which states that “[o]ne minister should be assigned the political responsibility for controlling and supervising internal security services, and his/[her] office should have full access in order to make possible effective day-to-day control. The minister should address an annual report to parliament on the activities of internal security services”.

⁶³ *Op. cit.* footnote 24, par 19 (2010 UN SRCT Compilation). See also Venice Commission-CoE Directorate of Human Rights (DGI), [Joint Opinion on the Draft Law no. 281 Amending and Completing Moldovan Legislation on the So-Called “Mandate of Security”](#), CDL-AD(2017)009, par 53. In a number of European states, to ensure that the head of the intelligence agency has a broad political backing, the competent parliamentary committees hold a hearing with a nominee and can issue a non-binding opinion or recommendation on the proposed appointment (e.g., in Estonia, Portugal, Hungary, and Croatia - see e.g., *op. cit.* footnote 24, pages 107-108 (2011 European

appointment modalities should aim to ensure greater transparency and merit-based appointment process, while ensuring some form of consultation with the Parliament guaranteeing wide political consensus.

46. As mentioned in Sub-Section 2.2 *supra*, SSU personnel are rights-holders and restrictions to their rights and freedoms should be strictly necessary and proportionate to ensure their political neutrality and impartiality and the proper performance of their duties. The partisan political participation and party membership of certain classes of public officials may be regulated or denied in order to ensure their impartiality and the proper functioning of their non-partisan public offices, and that they are able to fulfil their public functions free of a conflict of interest.⁶⁴ Some states have adopted specific measures restricting intelligence services' involvement in party politics e.g., prohibitions on accepting instructions or money from a political party, or from acting to further the interests of any political party.⁶⁵ It is also good practice to explicitly set legal limits to what the intelligence agencies can be asked to do, for instance prohibiting them from using their powers to target lawful political activity or other lawful manifestations of the rights to freedom of association, peaceful assembly and expression.⁶⁶ **The drafters could consider introducing provisions to that effect in the Draft Concept or relevant legislation.**

4. MANDATE, ACTIVITIES AND POWERS OF THE SSU

4.1. Mandate of the SSU

47. Section 5 of the Draft Concept provides an overview of the mandate and powers of the SSU. There is no binding international legal standard establishing the scope of mandate of security services. However, according to the *UN SRCT Compilation*, the main purpose of security services is generally to “[c]ollect, analyze and disseminate information that assists policymakers and other public entities in taking measures to protect national security”.⁶⁷ The *UN SRCT Compilation* further states that their “[m]andates are strictly limited to protecting legitimate national security interests as outlined in publicly available legislation or national security policies, and identify the threats to national security that intelligence services are tasked to address. If terrorism is included among these threats, it is defined in narrow and precise terms”.⁶⁸
48. In this context the way national security threats are defined in national legislation shapes the scope of the security services' mandates and it is therefore essential that national laws clearly define such terms (see *ODIHR Opinion on the Draft Amendments*).⁶⁹ The Law on

Parliament's [Study on the Parliamentary Oversight of Security and Intelligence Agencies in the EU](#)). For instance, in Croatia, the Director of the security service (SOA) is appointed by a decision co-signed by the President and the Prime Minister, for a four-year term, with possibility for renewal; the law additionally requires that the opinion of the Parliamentary Committee for Interior Policy and National Security is obtained (Article 66 (1) of the [Act on the Security and Intelligence System of the Republic of Croatia](#)); while the parliamentary committee does not have a formal veto power, a strongly articulated negative opinion of a candidate would damage the legitimacy of the President's and the PM's nomination. In Canada, the director of the intelligence agency is appointed for a five-year term, renewable only once, by the cabinet through a process known in Canada as Governor in Council (GIC) appointment, which is open to all Canadians, transparent and merit-based (see Canada, Security of Information Act (R.S.C., 1985, c. O-5), Section 4).

⁶⁴ See e.g., OSCE/ODIHR-Venice Commission, [Guidelines on Political Party Regulation](#) (2011), pars 117-118.

⁶⁵ *Op. cit.* footnote 24, par 19 (2010 UN SRCT Compilation).

⁶⁶ *ibid.* Practice 13 and par 20 (2010 UN SRCT Compilation); and par 150 (2015 Venice Commission [Report on the Democratic Oversight of the Security Services](#)).

⁶⁷ *Op. cit.* footnote 24, Practice 1 (2010 UN SRCT Compilation).

⁶⁸ *ibid.* Practice 2 (2010 UN SRCT Compilation).

⁶⁹ For example, in Canada, the Canadian Security Intelligence Service (CSIS) is mandated to “collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyze and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and, in relation thereto, shall report to and advise the Government of Canada” (see [Canadian Security Intelligence Service Act](#) (R.S.C., 1985, c. C-23), Section 12(1)). Additionally, Section 2 of the CSIS Act lists in detail what is meant by “threat to the security of Canada”: (a) espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage; b) foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person; (c) activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons

National Security of Ukraine (2018) does not provide an exhaustive list of constituting elements of “national security” or a definitive list of threats to national security. As per Article 3(5) of that Law, it is left to “the National Security Strategy of Ukraine, the Military Security Strategy of Ukraine, the Cyber Security Strategy of Ukraine, other documents on national security and defence approved by the National Security and Defence Council of Ukraine’ to determine the list of threats”. Such a scattered and open-ended approach to defining national security and threats thereto can lead to ever broadening mandate of the SSU.

49. In the absence of an exhaustive legal definition of national security and threats, the Draft Concept provides the SSU with the mandate as listed in Section 5.1, which *inter alia* includes the “fight against terrorism”. As per *UN Compilation of Good Practices*, when counter-terrorism is included in the mandate of security services, states shall “adopt legislation that provides precise definition of terrorism as well as terrorist groups and activities”.⁷⁰ The analysis of the Ukrainian definition of “terrorism” goes beyond the scope of this Opinion. At the same time, and while acknowledging that there is no internationally-agreed definition of terrorism,⁷¹ it is important to reiterate that the national legislation shall provide for a clearly and strictly circumscribed definition of “terrorism” that is human rights-compliant and complies with the principles of legal certainty, foreseeability and specificity of criminal law (see *ODIHR Opinion on the Draft Amendments*).⁷²
50. As it stands, the Draft Concept refers to SSU’s role to fight organized crime, corruption and economic crimes (Section 3.1, 7th indent), and to implement measures to counteract cybercrimes (Section 5.3, 9th indent). Generally, **the SSU should not be involved in the fight against such crimes, unless these pose a clear and present danger to national security.**⁷³ **This caveat should be expressly mentioned in the Draft Concept, if the SSU remains entrusted with such functions at all.**
51. It is important to emphasize however that **cybersecurity⁷⁴ as opposed to cybercrimes should be part of SSU’s mandate.** Indeed, it is legitimate and in line with international practices to have security and intelligence services protect critical infrastructure and government ICT systems from attacks, including the breach of sensitive data affecting public safety and national security.
52. In light of the foregoing, the drafters should **reconsider SSU’s mandate concerning the fight against organized crime, corruption, economic crimes and cybercrimes, or specify that SSU is involved only when these crimes pose a clear and present danger to national security.** More generally, **Ukraine should revise the mandate of the SSU, linking it to the protection of national security. The constituting elements and threats**

or property for the purpose of achieving a political, religious or ideological objective within Canada or a foreign state, and; d) activities directed toward undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of, the constitutionally established system of government in Canada”.

⁷⁰ *Op. cit.* footnote 24, Practice 2 and par 10 (2010 UN SRCT Compilation).

⁷¹ UN Special Rapporteur on counter-terrorism, [2005 Report](#), UN Doc. E/CN.4/2006/98, pars 26-28; [2010 Report on Ten areas of best practices in countering terrorism](#), UN Doc. A/HRC/16/51 (2010), pars 26-28; and 2019 [Report to the UN Commission on Human Rights](#), UN Doc. A/HRC/40/52, 1 March 2019, par 19.

⁷² This requires that criminal offences and related penalties be defined clearly and precisely, so that an individual knows from the wording of the relevant criminal provision which acts will make him/her criminally liable. In that respect, the UN Special Rapporteur on counter-terrorism has noted that any definition of terrorism would require three cumulative elements to be human rights-compliant i.e., it should amount to an action: (1) corresponding to an offence under the universal terrorism-related conventions (or, in the alternative, action corresponding to all elements of a serious crime defined by national law); **and** (2) done *with the intention* of provoking terror or compelling a government or international organization to do or abstain from doing something; **and** (3) passing a certain threshold of seriousness, i.e., either (a) amounting to the intentional taking of hostages, or (b) intended to cause death or serious bodily injury, or (c) involving lethal or serious physical violence. It is worth emphasizing that the UN Special Rapporteur on counter-terrorism has also expressly stated that “[d]amage to property, absent other qualifications, must not be construed as terrorism” - see UN Special Rapporteur on counter-terrorism, [2010 Report](#), A/HRC/16/51, 22 December 2010, par 27; [2019 Report](#), par 75 (c); **and UN Security Council Resolution 1566 (2004)**, S/RES/1566 (2004), par 3. See also OSCE TNTD-SMPU and ODIHR [Preventing Terrorism and Countering VERT](#) (2014), pages 27-30; and ODIHR, [Guidelines on Addressing the Threats and Challenges of “Foreign Terrorist Fighters”](#) (2018), Chapter 3.1.

⁷³ See e.g., *op. cit.* footnote 24, par A.2 (1999 PACE Recommendation 1402).

⁷⁴ See the definition of “cybersecurity” contained in 2010 Resolution 181 of the UN International Telecommunication Union (ITU).

to national security should be clearly and exhaustively defined by law. In respect to the counter-terrorism mandate of the SSU, the Draft Concept should make clear references to national laws which define terrorism and terrorist acts, groups and activities, and specify that a review of such offences should be carried out to ensure full compliance with international human rights standards and recommendations.

KEY RECOMMENDATION A.1.

To reconsider SSU's mandate concerning the fight against organized crime, corruption, economic crimes and cybercrimes, or specify that SSU is involved only when these crimes pose a clear and present danger to national security, and more generally ensure that SSU's mandate is systematically linked to the protection of national security, while ensuring that the constituting elements and threats to national security are strictly, clearly and exhaustively defined.

53. Sections 1.1 and 2.1 refer to the SSU as a “*special-purpose state body with law enforcement functions*”. This definition is vague, categorizing the SSU somewhere between a domestic security service and a law enforcement agency. Sections 3.1, 2nd indent, and 5.2, last indent, provide SSU with “*pre-trial investigation of crimes*”, which is a typical law enforcement task. Section 3.1, 8th indent, states that “*the participation of the SSU in the investigation of economic, corruption and other crimes not belonging to its jurisdiction shall be made impossible*”, while Section 5.5 specifies that such powers should be delegated to other state bodies during 2020-2027. However, it remains rather unclear which crimes will remain within the SSU's competence, apart from the express reference to terrorism and cyber-crime (see Section 5.3 of the Draft Concept).
54. Such an amalgamation of functions is not in line with international standards and good practices, which call for a separation between intelligence and law enforcement functions, to avoid risk of abuse of these powers.⁷⁵ Section 3.1, 5th indent, states that the “*activity of the SSU will be shifted from law-enforcement to counter-intelligence*”, which appears in line with international recommendations and good practices. At the same time, it appears from other provisions of the Draft Concept that the SSU will retain some law enforcement functions. Indeed, the law enforcement tasks of the SSU will be reduced to “*limited law enforcement functions in the field of state security*” (Section 8.5 of the Draft Concept), which will still include typical enforcement tasks such as the “*pre-trial investigation of crimes*”(Section 5.2). **It is recommended to systematically remove any law**

⁷⁵ *Op. cit.* footnote 24, par 41 (2010 UN SRCT Compilation). See also e.g., *op. cit.* footnote 24, par B.3 (1999 PACE Recommendation 1402), which states that “[i]nternal security services should not be authorised to carry out law-enforcement tasks such as criminal investigations, arrests, or detention. Due to the high risk of abuse of these powers, and to avoid duplication of traditional police activities, such powers should be exclusive to other law-enforcement agencies”; and *op. cit.* footnote 24, page 28 (2017 EU FRA Surveillance by Intelligence Services), in which the EU FRA concluded, based on a survey of intelligence services across the EU, that the “*separation between security services and law enforcement agencies is regarded as a strong safeguard against too much concentration of power in one service, and the risk of arbitrary use of intelligence collected through covert methods*”. As examples of recognized country good practices: in Canada, the Law on Canadian Intelligence Service explicitly bans the use of any law enforcement power (Section 12.1(1) of the Canadian Security Intelligence Service Act defines the powers of the service as follows: “*If there are reasonable grounds to believe that a particular activity constitutes a threat to the security of Canada, the Service may take measures, within or outside Canada, to reduce the threat*”; however, the Section explicitly states: “*For greater certainty, nothing in subsection (1) confers on the Service any law enforcement power*”; in addition to explicitly prohibiting CSIS from using police powers, section 12.2(1) stipulates further prohibited conduct by stating: “*the Service shall not: (a) cause, intentionally or by criminal negligence, death or bodily harm to an individual; (b) willfully attempt in any manner to obstruct, pervert or defeat the course of justice; or (c) violate the sexual integrity of an individual*”; in Germany, the legislation tends to create a clear demarcation between the domestic intelligence service and law enforcement agencies (the domestic security service of Germany (BfV) is not given the powers to conduct criminal investigations and exercising law enforcement powers; also, it cannot order the police to carry out arrests on its behalf; however, the BfV law outlines in detail the specific and circumstances under which the BfV is allowed to share information with law enforcement agencies (see <<https://www.gesetze-internet.de/bverfschg/>>. Articles 20-23 of the Law).

enforcement functions, such as criminal investigations, arrest and detention, from the scope of the powers of the SSU and transfer them to the police and the prosecutorial/judicial authorities, as appropriate, thus focusing exclusively on intelligence/counter-intelligence activities. If entrusting the SSU with law enforcement powers is nevertheless deemed an absolute necessity, then the scope and application of such powers should be strictly limited as further detailed below.

55. First, such law enforcement powers should only be used within the context of a mandate that gives them the responsibility for countering specific and strictly limited national security threats, which may include terrorism⁷⁶ but not, as mentioned above, other general crimes such as organized crime, corruption, economic crimes and cybercrimes, unless these pose a clear and present danger to national security. From the broad wording of the Draft Concept, it is not clear **for which criminal offences threatening national security the SSU would be able to resort to law enforcement powers and this should be clarified.**
56. Second, the policy and legal framework should ensure that there are no other law enforcement bodies having a mandate to enforce criminal law in relation to the same “*national security offences*”. In summary, there should be no duplication of law enforcement powers between the SSU and other state agencies or bodies for addressing the same activities.⁷⁷ In that respect, it is somewhat welcome that Section 1.4 specifically states the objective of eliminating the “*redundancy of competencies with other law enforcement agencies*”. At the same time, in substance, the Draft Concept seems to retain the SSU’s competence for the investigation of potentially any crime (Section 3.1, 8th indent). **It is therefore recommended to include a clear statement that if SSU’s law enforcement powers are retained at all, other law enforcement bodies shall not exercise law enforcement powers in relation to the same criminal offences.**
57. Similarly, Section 5.3, 12th indent, should clarify what is meant by “*pre-trial investigation of criminal offences belonging to the competence of security authorities*”, while ensuring that the SSU is not given the power to investigate other crimes under the mandate of other security and law enforcement agencies.
58. Third, the exercise of these powers by the SSU should be subject to the same legal safeguards and oversight that apply to other law enforcement agencies,⁷⁸ and it is recommended to clearly state this principle in the Draft Concept. The Draft Concept, and the subsequent legal amendments, should clearly define and regulate the use of SSU’s law enforcement powers, if these are retained at all, including whether or not they entail the use of lethal force, arrest and detention. According to the current Law on the SSU, Article 26 gives the SSU staff the powers to use weapons and other means of force on an equal basis with the National Police of Ukraine, without any special restriction on SSU staff using lethal force. As such, they should comply with international standards and recommendations, including Article 6 of the ICCPR, Article 2 of the ECHR, the [UN Code of Conduct for Law Enforcement Officials](#) (1979) and the [UN Basic Principles on the Use of Force and Firearms by Law Enforcement Officials](#) (1990). There is also no stipulation in the Law on how SSU can carry out arrest and detention, other than a reference to SSU carrying out operational activities in accordance with the Law of Ukraine on Detective Investigation Activity (as per Article 25(8)). There is a large body of legal and normative standards applicable to arrest and detention, including Article 9 of the ICCPR, Article 5 of ECHR, as well as the [UN Standard Minimum Rules for the Treatment of Prisoners](#) (2015), though this goes beyond the scope of this Opinion. In any case, the

⁷⁶ *Op. cit.* footnote 24, par 41 (2010 UN SRCT Compilation).

⁷⁷ *Op. cit.* footnote 24, Practice 27 and par 41 (2010 UN SRCT Compilation).

⁷⁸ *Op. cit.* footnote 24, Practice 28 (2010 UN SRCT Compilation).

SSU is not permitted to deprive persons of their liberty simply for the purpose of intelligence collection.⁷⁹ Arrest and detention by intelligence services is subject to the same degree of oversight as applies to their use by law enforcement authorities, including judicial review of the lawfulness of any deprivation of liberty.⁸⁰ The SSU should also not be permitted to operate its own detention facilities or to make use of any unacknowledged detention facilities operated by third parties.⁸¹ **All these limitations and safeguards should be reflected in relevant legislation.**⁸²

59. Fourth, the SSU law enforcement powers should be restricted to cases in which there is a reasonable suspicion that an individual has committed or is about to commit a specific national security criminal offence or related preparatory/inchoate offences.⁸³

KEY RECOMMENDATION A.2.

To ensure that, throughout the Draft Concept, SSU's mandate is limited to intelligence/counter-intelligence activities and remove any law enforcement functions, such as criminal investigations, arrest and detention, from the scope of the powers of the SSU and transfer them to the police and the prosecutorial/judicial authorities, as appropriate; or if deemed an absolute necessity and retained, strictly limit the scope and application of such law enforcement powers exclusively for combatting certain clearly defined national security criminal offences, when there is a reasonable suspicion that an individual has committed or is about to commit such offences or related preparatory/inchoate offences; specify that other law enforcement bodies shall not exercise law enforcement powers in relation to the same offences; and ensure that the exercise of these powers by the SSU is subject to the same legal safeguards and oversight that apply to other law enforcement agencies.

60. Finally, Section 5.4 of the Draft Concept specifies that “*information obtained as a result of counter-intelligence and intelligence activities shall not be used to solve criminal proceedings other than in the manner provided in the Law of Ukraine On Counter-Intelligence Activities*”. This provides a safeguard by attempting to separate the use of information obtained as part of counter-intelligence, and information used in the context of criminal investigations. However, the provision does not elaborate on how this separation will be regulated in practice and overseen by the respective oversight actors. **The Draft Concept should be supplemented in that respect.**

4.2. Operational and Search Activity

61. Section 5.2, 3rd indent, refers to “*operational and search activity*” carried by the SSU. Section 5.3, 14th indent, refers to “*special technical means for retrieving information from communication channels and other technical means of covert collection of information*” and to the “*direct use of technical means for covert search, control, selection, recording and processing of data within the framework of operational and counter-intelligence cases and criminal proceedings*”.

⁷⁹ *ibid.* Practices 28 and 30 (2010 UN SRCT Compilation).

⁸⁰ *ibid.* Practices 28 and 30 (2010 UN SRCT Compilation).

⁸¹ *ibid.* Practices 28 and 30 28 (2010 UN SRCT Compilation).

⁸² See *op. cit.* footnote 1, especially the Sub-Section on the Powers of the SSU (2020 ODIHR Opinion on the Draft Amendments).

⁸³ *ibid.* Practice 28 (2010 UN SRCT Compilation).

62. The state acquisition and recording of information on individuals obtained through surveillance, interception of communication or undercover operations have the potential to severely encroach on human rights and fundamental freedoms. It is therefore important that such surveillance activities are carried out with due regard to the principles of legality, necessity and proportionality, while being subject to judicial control, and that the state ensures the utmost transparency about the legal basis, scope and modalities of such measures and methods.⁸⁴ Moreover, such investigative actions shall, in light of their intrusive character, the lack of public scrutiny and the ensuing risk of misuse of power, be subject to extremely strict conditions and safeguards.⁸⁵ **It is recommended that such caveat be expressly mentioned in the Draft Concept, while providing that the legal framework for carrying such operational and search activities should be reviewed to ensure compliance with international human rights standards** (see also *ODIHR Opinion on the Draft Amendments* which further details the conditions and circumstances for using such measures).
63. It is not clear from the Draft Concept whether the SSU will be conducting not only targeted surveillance but also potentially strategic (mass) surveillance, which also constitutes a high risk for violations of human rights, particularly the right to respect for private and family life. As appropriate, **the Draft Concept, as well as the subsequent law, should clearly state that the SSU’s powers to conduct such surveillance, should be in line with international human rights standards and that the underlying legal framework should be reviewed to ensure compliance with such standards** (see also the *ODIHR Opinion on the Draft Amendments*).
64. Finally, Section 5.3, 14th indent, details the surveillance activities. It seems to give the SSU the monopoly in implementing covert surveillance measures to be used by all law enforcement bodies in the criminal justice system. If this is the case, then the **Draft Concept and subsequent laws should put in place effective safeguards to make sure that there is a separation between (untargeted) “strategic surveillance” conducted for intelligence purposes⁸⁶ and targeted surveillance conducted for criminal investigations** (whereby higher levels of legal safeguards and control apply), **though the policy-makers may seek to apply or adapt the more stringent safeguards to “strategic surveillance”** (see also *ODIHR Opinion on the Draft Amendments*).

4.3. Data Collection and Processing

65. Section 3.1, 12th indent, refers to the provision of “*necessary operational, technical and organisational capabilities for obtaining operational information*”. The collection, processing and sharing of information, including personal data, is a core task of security services and one that carries substantial risk of violating human rights, particularly the right to respect for private and family life, protected by Article 17 of the ICCPR and Article 8 of the ECHR. **It is therefore essential that the Draft Concept explicitly makes necessary references to such international standards on the right to respect for private and family life, including to judicial oversight and effective mechanisms for data protection.**
66. Additionally, **the Draft Concept should also refer to relevant standards on the processing of personal data, including the *Council of Europe Convention for the***

⁸⁴ See UN Special Rapporteur on freedom of opinion and expression, *2013 Report*, pars 91-92, which notes how important it is for States to be transparent about the use and scope of communications surveillance techniques and powers, particularly in relation to internet service providers. See also *op. cit.* footnote 24., Principle 10.E (2013 Tshwane Principles).

⁸⁵ See ECtHR, *Uzun v. Germany* (Application no. 35623/05, judgment of 2 September 2010), par 63.

⁸⁶ *Op. cit.* footnote 24, par 52 (Venice Commission *2015 Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Agencies*).

Protection of Individuals with regard to Automatic Processing of Personal Data,⁸⁷ though the Convention permits derogations from certain principles in the Convention in the interest of national security providing that they are lawful, necessary and proportionate. Additional recommendations on these aspects are provided in the *ODIHR Opinion on the Draft Amendments*.

4.4. Information Exchange and Co-operation with Foreign Security Services

67. Section 3.1, 20th and 21st indents, refer to information exchange with other countries and to the “*interaction with partner special services of foreign countries and international security institutions*”. Generally, co-operation between security services may risk circumventing the existing national mechanisms of control.⁸⁸ To prevent such risks, **it is important that the Draft Concept states that subsequent legislation shall provide adequate safeguards in relation to international co-operation, in line with international standards and good practices, and shall not be used to circumvent national standards and institutional controls and should not ultimately result in potential human rights violations** (see more detailed recommendations in that respect in the *ODIHR Opinion on the Draft Amendments*).⁸⁹

4.5. Other Comments

68. Section 5.3 of the Draft Concept details the types of activities that the SSU can carry out, in view of its mandate and powers and all the recommendations made above are relevant to this Section too. In addition, Section 5.3 refers to the “*prevention and suspension of activities of international terrorist organizations in the territory of Ukraine*”. **To avoid abuse, it is important to define the list of international terrorist organisations, as recognized by Ukraine, in a publicly available law promulgated by the Parliament** (additional recommendations are provided in that respect in the *ODIHR Opinion on the Draft Amendments*).
69. Section 5.3, 7th indent, refers to “*other groups and associations whose activities pose a threat to national security*”. Such a wording is overly vague and broad and may result in arbitrary expansion of SSU’s mandate if threats to national security are not strictly defined by law. This broad terminology cannot exclude that this may lead to abuse against certain associations carrying out legitimate activities that may appear offensive or that defend positions that may “*offend, shock or disturb*” the State or any part of the population.⁹⁰ As stated in the OSCE/ODIHR-Venice [Commission Guidelines on Freedom of Association](#), the rights to freedom of expression and to freedom of association entitle associations to pursue objectives or conduct activities that are not always congruent with the opinions and beliefs of the majority or run precisely counter to them.⁹¹ This includes e.g., “*imparting information or ideas contesting the established order or advocating for a peaceful change of the Constitution or legislation by, for example, [...] asserting a minority consciousness, [...] calling for regional autonomy, or even requesting secession of part of the country’s territory*”.⁹² **To avoid any risk of abuse, the wording “other groups and associations whose activities pose a threat to national security” should be removed and the law**

⁸⁷ Council of Europe, [Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data](#), CETS No. 108, which entered into force in Ukraine on 1 January 2011.

⁸⁸ See e.g., *op. cit.* footnote 24, par 74 (2015 Venice Commission’s [Report on the Democratic oversight of Signals Intelligence Agencies](#)).

⁸⁹ *Op. cit.* footnote 24, Practices 31-35 (2010 UN SRCT Compilation). See also ODIHR, [Guidelines on Addressing the Threats and Challenges of “Foreign Terrorist Fighters”](#) (2018), page 43; and *op. cit.* footnote 24, par 75 (2015 Venice Commission’s [Report on the Democratic oversight of Signals Intelligence Agencies](#)); and Recommendation 5 (2015 CoE Commissioner for Human Rights [Democratic and Effective Oversight of National Security Services](#)).

⁹⁰ UN Special Rapporteur on counter-terrorism, [2015 Thematic Report](#), A/HRC/31/65, 22 February 2016,

⁹¹ ODIHR-Venice Commission, [Guidelines on Freedom of Association](#) (2015), par 182.

⁹² ODIHR-Venice Commission, [Guidelines on Freedom of Association](#) (2015), par 182.

should in the future define and make an exhaustive list of illegal armed and paramilitary formations that the SSU is expected to counteract and counter-sabotage.

5. CONTROL AND OVERSIGHT OVER THE ACTIVITIES OF THE SECURITY SERVICE OF UKRAINE

70. Section 8 of the Draft Concept provides an overview of the mechanisms of control and oversight mechanisms, which is welcome. Indeed, according to the 1994 [OSCE Code of Conduct on Politico-Military Aspects of Security](#), OSCE participating States “*consider the democratic political control of military and paramilitary forces as well as the activities of the internal security and intelligence services to be an indispensable element of stability and security*” (par 20).
71. The Draft Concept repeatedly affirms the importance of “*democratic civilian control*” and the SSU’s commitment to it (see e.g., Section 1.4. last indent and Section 2.2. last indent), but in most cases, it does not elaborate the specific measures to improve such democratic control. The scope, mandate and powers of oversight mechanisms remain unclear in the Draft Concept. While it is welcome to have a separate Chapter in the Draft Concept on control and oversight, if the respective provisions are not further operationalized through being elaborated in the Concept and/or future amendments to the Law on the Security Service of Ukraine, oversight bodies risk to remain inoperative.
72. International recommendations and good practices call for a multilevel system of internal, executive, parliamentary, judicial, specialized and public oversight mechanisms.⁹³ The combined remit of oversight institutions should cover all aspects of the work of intelligence services, including **their compliance with the law and international human rights standards, the effectiveness and efficiency of their activities, their finances and their administrative practices**.⁹⁴ As such, oversight should not only focus on the “*activities of the SSU*” as stipulated, for instance, in Section 8.1. of the Draft Concept, but all such aspects of the SSU’s functioning and work. **The Draft Concept should be supplemented in that respect**. Also, all the principles referred to in Section 3 *supra* should guide the reform process when it comes to internal and external oversight.
73. Additionally, it is essential that **oversight be gender- and diversity-sensitive and this should be expressly stated in the Draft Concept**. This means that oversight bodies should be concerned with how security services are pursuing gender equality goals; ensure that their approach to national security, as well as laws and regulations, reflect the security needs of all individuals, taking into account their diversity; and more generally that they are working towards the Women, Peace and Security Agenda.⁹⁵ The composition of oversight bodies should be diverse and inclusive. Oversight bodies should also have appropriate mandates, powers and resources to enable them to undertake a systemic examination of gender and diversity issues both regarding internal intelligence services’ functioning and staffing and when they carry out their activities.⁹⁶ They should take steps to build their own internal institutional capacity to address gender and diversity issues and integrate a gender and diversity perspective, including through training and developing mechanisms to access expert advice⁹⁷, and ensure allocations of human and financial resources to this end. If they have power to receive complaints, they should ensure that

⁹³ *Op. cit.* footnote 24, Practice 6 (2010 UN SRCT Compilation); page 58 (2015 CoE Commissioner for Human Rights [Democratic and Effective Oversight of National Security Services](#)); par 7 (2015 Venice Commission’s [Report on the Democratic Oversight of the Security Services](#)); and page 28 (2017 EU FRA Surveillance by Intelligence Services).

⁹⁴ *ibid.* Practice 6 (2010 UN SRCT Compilation).

⁹⁵ *Op. cit.* footnote 25, page 21 (2019 DCAF-OSCE/ODIHR-UN Women Tool no. 14 on Intelligence and Gender).

⁹⁶ *ibid.* page 33 (2019 DCAF-OSCE/ODIHR-UN Women Tool no. 14 on Intelligence and Gender).

⁹⁷ *ibid.* page 33 (2019 DCAF-OSCE/ODIHR-UN Women Tool no. 14 on Intelligence and Gender).

their receipt, handling and investigations of complaints – for people within the services and for any individual wishing to file a complaint against the intelligence service – are non-discriminatory, gender- and diversity-responsive and accessible.⁹⁸ **Such aspects should be reflected under Section 8 of the Draft Concept.** In that respect, the [2019 DCAF-OSCE/ODIHR-UN Women Tool no. 7 on Parliamentary Oversight of the Security Sector and Gender](#) can serve as a useful reference tool.

74. All oversight bodies, including parliament, ombuds institutions, courts, tribunals and appellate bodies, should also have a right to access to all (classified) information relevant to their functions and necessary for discharging their responsibilities on the basis of procedure clearly defined by law.⁹⁹ **It is important that the Draft Concept clearly state such a principle.** In support of this, the SSU should be obliged to keep detailed records and to disclose to oversight bodies any material requested.¹⁰⁰ An oversight body of which the functions include reviewing questions of legality, effectiveness and respect for human rights will require access to even more specific information.¹⁰¹ Also, oversight bodies should have access to the necessary financial, technological, and human resources to enable them to identify, access, and analyze information that is relevant to the effective performance of their functions.¹⁰²

KEY RECOMMENDATION B.

To ensure that oversight not only focuses on the “*activities of the SSU*” but covers all aspects of the SSU’s functioning and work, while defining more clearly the scope, mandate and powers of the different control and oversight mechanisms and guaranteeing that they all have a right to access to all (classified) information relevant to their functions and necessary to discharge their responsibilities on the basis of procedure clearly defined by law.

5.1. Internal Control

75. Section 8 of the Draft Concept does not refer to internal control, apart from a rather generic reference to an “*optimized system of intra-departmental control*” (Section 8.1, last sentence). In principle, the management of security services itself should ensure that the services operate in compliance with laws and human rights standards, should provide relevant direction, guidance and qualitative training in this respect as well as carry out necessary internal disciplinary investigations for misconduct.¹⁰³ This type of internal control can be carried out either through dedicated units or by establishing inspectorate generals.¹⁰⁴ Moreover, as further developed in par 92 *infra*, it is important to set up proper and functioning internal reporting, complaint and accountability mechanisms, with adequate allocation of human and financial resources. **In this respect, it is recommended**

⁹⁸ *ibid.*, page 33 (2019 DCAF-OSCE/ODIHR-UN Women Tool no. 14 on Intelligence and Gender).

⁹⁹ *Op. cit.* footnote 24, par 98 (2015 Venice Commission’s [Report on the Democratic Oversight of the Security Services](#)); 49-50 (2015 CoE Commissioner for Human Rights [Democratic and Effective Oversight of National Security Services](#)); and Principle 6 (2013 Tshwane Principles).

¹⁰⁰ See e.g., European Parliament, [Resolution on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens’ fundamental rights and on transatlantic cooperation in Justice and Home Affairs](#), adopted by the European Parliament on 12 March 2014 (2013/2188(INI)).

¹⁰¹ See e.g., Venice Commission, [2007 Report on the Democratic Oversight of the Security Services](#), par 163.

¹⁰² *Op. cit.* footnote 24, Principle 33 (2013 Tshwane Principles).

¹⁰³ *Op. cit.* footnote 24, page 58 (2015 CoE Commissioner for Human Rights [Democratic and Effective Oversight of National Security Services](#)); and par 15 (2015 Venice Commission’s Report on the Democratic Oversight of the Security Services).

¹⁰⁴ *ibid.*

to include in the Draft Concept a reference to internal control mechanisms within the SSU, and what this would imply.

5.2. Executive Control

76. As per Section 8.1, 1st indent, the executive control will be exercised by the President of Ukraine, the National Security and Defence Council and the Presidential Ombudsman. **It would be advisable to elaborate what kind of role and control is foreseen by each of those executive actors beyond appointment and dismissal of the Head of the SSU.**

5.3. Parliamentary Oversight

77. Section 8.1, 2nd indent, refers to parliamentary oversight by the Verkhovna Rada of Ukraine in terms of law-making concerning the regulation of the activities of the SSU, its powers, budget and reporting) and by the Parliamentary Committee of the Verkhovna Rada controlling the activities of special purpose bodies. It further refers to the Parliament Commissioner for Human Rights of the Verkhovna Rada for overseeing the observance of human rights and freedoms by the SSU. While it is good practice that a Parliamentary Committee of the Verkhovna Rada is mandated to oversee the SSU,¹⁰⁵ it is important that such a committee be granted special powers to oversee security and intelligence agencies, including access to confidential or classified information, the ability to launch parliamentary investigations and summon SSU management for a hearing, and the handling of petitions.¹⁰⁶ **The Draft Concept should mention that the said committee should be granted such special powers and access to confidential/classified information, as detailed in the subsequent law** (for further details see the *ODIHR Opinion on the Draft Amendments*).

5.4. Parliament Commissioner for Human Rights

78. Section 8.1, 2nd indent, refers to the Parliament Commissioner for Human Rights of the Verkhovna Rada, to control the observance by the SSU of constitutional human and civil rights and freedoms. This is in line with the PACE recommendations which state that “[o]ther bodies (for example ombudsmen and data protection commissioners) should be allowed to exercise ex post facto control of the security services on a case-by-case basis”.¹⁰⁷ **It is however essential that the Draft Concept, or a subsequent law refers to the scope, mandate and powers of Parliament Commissioner for Human Rights in overseeing the SSU.**
79. Beyond such oversight, it is an established good practice among European countries to set up an expert body exclusively dedicated to intelligence service oversight with powers such as authorising surveillance measures, investigating complaints, requesting documents and information from the intelligence services, or giving advice to the executive and/or parliament.¹⁰⁸ Across the European Union, 15 countries have established such expert

¹⁰⁵ *Op. cit.* footnote 24, par 15d (2005 PACE Recommendation 1713), which states that “the control of activities of special services should be carried out by a special parliamentary committee”.

¹⁰⁶ *Op. cit.* footnote 24, pages 34-35 (2017 EU FRA Surveillance by Intelligence Services).

¹⁰⁷ *Op. cit.* footnote 24, par C.4 (1999 PACE Recommendation 1402).

¹⁰⁸ Among those European countries, Germany and Belgium have set-up powerful expert oversight bodies, namely the G-10 Committee in Germany and the Standing Intelligence Oversight Committee (Committee I) and Administrative Commission in Belgium. The Committee I in Belgium (i) reviews and provides advice on laws, or any other policy documents relating to the governance of security services, while also providing written advice to the judicial authorities on the legality of the way in which information added to criminal proceedings was collected by the intelligence and security services; (ii) conducts ex-post oversight of the implementation of targeted surveillance measures, while the Administrative Commission is in charge of ex-ante authorisations; (iii) oversees strategic surveillance conducted abroad by the military intelligence agency and also oversees the security services’ cooperation with their international counterparts, which is a novel approach among expert oversight bodies; (iv) upon complaints, requests by the Parliament or judicial authorities, carries out investigations, including investigations against members of the services who are suspected of having committed a felony or misdemeanour, in a judicial

oversight bodies.¹⁰⁹ In future stages of the SSU reform, **Ukrainian authorities could consider establishing such an expert oversight body, with exclusive mandate on overseeing the SSU, in particular its covert surveillance and operative activities.**

5.5. Judicial Accountability

80. Section 8.1, 3rd indent, states that “*the judicial bodies of Ukraine*” will carry out control over the activities of the SSU. However, it is not clear what this would imply. The Parliamentary Assembly of the Council of Europe clearly states that “[*t*]he judiciary should be authorised to exercise extensive *a priori* and *ex post facto* control” over intelligence services.¹¹⁰ This should include prior judicial authorization to carry out certain operative/investigative activities with a high potential to infringe upon human rights. Moreover, people who feel that their rights have been violated by the SSU should also be able to seek redress before courts. Should the SSU retain law enforcement functions, it is worth emphasizing that the OSCE participating States have committed in the [OSCE Moscow Document](#) (1991) to “*ensure that law enforcement acts are subject to judicial control, that law enforcement personnel are held accountable for such acts, and that due compensation may be sought, according to domestic law, by the victims of acts found to be in violation of the above commitments*”.¹¹¹
81. **It would be advisable that the Draft Concept or a subsequent law stipulates the scope and extent of judicial oversight, both in term of *a priori* and *ex post facto* control. This should include in particular the ex-ante authorisation of surveillance, the ongoing oversight of information collection measures (supervision of investigations, ordering the termination of surveillance and ordering the destruction of data collected) and ex-post adjudication of cases (see also Sub-Section 5.7 *infra*).**¹¹²

KEY RECOMMENDATION C.

To stipulate the scope and extent of judicial oversight, both in term of *a priori* and *ex post facto* control, in particular the *ex-ante* authorization of surveillance, the ongoing oversight of information collection measures and *ex-post* adjudication of cases.

5.6. Public Oversight

82. In Section 8.3, the Draft Concept states that “*the mass media, non-government organizations and individual citizens shall participate in exercising public control over the activities of the Security Service of Ukraine*” in accordance with the procedure established by the Constitution and other laws. Furthermore, according to Section 8.3, “*in compliance with the current legislation on classified information, [the Security Service of Ukraine] shall publish information on the directions of its activity and its main results during the period under report (White Paper)*”. It is worth emphasizing that pursuant to Recommendation 1402 (1999) of the Parliamentary Assembly of the Council of Europe, “[*i*]ndividuals should be given a general right of access to information gathered and stored by the internal security service(s), with exceptions to this right in the interest of

capacity; and (v) serves as an appeal body for security clearances (see <<https://www.comiteri.be/index.php/en/standing-committee-i/eight-assignments>>).

¹⁰⁹ *Op. cit.* footnote 24, page 43 (2017 EU FRA Surveillance by Intelligence Services).

¹¹⁰ *Op. cit.* footnote 24, par C.3 (1999 PACE Recommendation 1402).

¹¹¹ CSCE/OSCE, [Document of the Moscow Meeting of the Conference on the Human Dimension of the CSCE](#), 3 October 1991, par 21.2.

¹¹² See e.g., Venice Commission, [Report on the Democratic oversight of Signals Intelligence Agencies](#), CDL-AD(2015)011, pars 105-106.

national security clearly defined by law. It would also be desirable that all disputes concerning an internal security service's power to bar disclosure of information be subject to judicial review".¹¹³ **The Section 5.3 of the Draft Concept could be supplemented in that respect, while specifying that aspects related to access to information and judicial review in case of SSU's refusal to disclose information should be detailed in a law** (see also recommendations on this aspect in the *ODIHR Opinion on the Draft Amendments*).

5.7. Prosecutor's Office's Supervision of Covert and Other Investigative and Search Actions

83. Section 8.2 states that the Prosecutor's Office of Ukraine will supervise "*covert and other investigative and search actions of the Security Service of Ukraine in accordance with the Constitution of Ukraine*". It is worth emphasizing that the ECtHR generally considers that there should be a judicial or independent control over the collection and use of collected information and, in that respect, the Prosecutor's Office may not be considered to be independent from the executive.¹¹⁴ **The drafters should ensure that judicial authorities carry out such supervision, instead or in addition to the Prosecutor's Office.**
84. Finally, as per the ECtHR case law, the power to order the immediate termination of surveillance measures when a violation by security services is identified is essential for an effective oversight system,¹¹⁵ and **this should also be reflected in the Draft Concept or relevant legislation.**

6. GENDER AND DIVERSITY CONSIDERATIONS AND NON-DISCRIMINATION

85. Gender and diversity considerations are only mentioned in relation to the development of effective staffing mechanism in line with standards on gender equality (Section 3.1, 15th indent) with the ultimate aim of creating equal recruitment and promotion opportunities for women and men and "*representatives of different groups and different regions of Ukraine*" (Section 6, 5th indent).
86. Achieving greater gender balance and diversity within the workforce of the SSU is a welcome objective as security sector institutions should be representative of the population they serve.¹¹⁶ At the same time, gender and diversity considerations in the context of SSR should go further and not be limited to merely increasing the representation of women and of different groups within security institutions. Indeed, gender equality and diversity should also be promoted internally as part of the working culture of the institution, as well as externally when delivering security services, while ensuring that security and justice are understood and addressed with a gender and diversity perspective.¹¹⁷ Additionally, CEDAW Committee [*General Recommendation no. 30 on Women in Conflict Prevention, Conflict and Post-conflict Situations*](#) (2013) specifically recommends that states undertake gender-sensitive and gender-responsive SSR. This should result in representative security sector institutions that address women's different security experiences and priorities, while ensuring that SSR is subject to inclusive oversight and accountability mechanisms with

¹¹³ *Op. cit.* footnote 24, par C.5 (1999 PACE Recommendation 1402). See also ODIHR, [*Guidelines on the Protection of Human Rights Defenders*](#) (2014), pars 145-148.

¹¹⁴ See e.g., ECtHR, [*Popescu v. Romania*](#) (Application no. 71525/01, 26 April 2007); and [*Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*](#) (Application no. 62540/00, judgment of 28 June 2007).

¹¹⁵ ECtHR, [*Roman Zakharov v. Russia*](#) [GC] (Application no. 47143/06, judgment of 5 December 2015), par 28.

¹¹⁶ DCAF-UNDP, [*Public Oversight of the Security Sector - A Handbook for Civil Society Organizations*](#) (2008), page 216.

¹¹⁷ *Op. cit.* footnote 25, Section 3 (2019 DCAF-OSCE/ODIHR-UN Women Tool no. 1 on SSG/SSR and Gender); and page 16 (2019 DCAF-OSCE/ODIHR-UN Women Tool no. 14 on Intelligence and Gender).

sanctions, and strengthening gender expertise and the role of women in oversight of the security sector.¹¹⁸

87. It is thus essential to adopt policy frameworks to integrate gender equality and diversity into justice and security governance,¹¹⁹ and that gender and diversity considerations are an integral part of all the dimensions of the SSU's reform. The following paragraphs will explain the practical implications of such an effort.
88. First, and as mentioned in Sub-Section 2.1 *supra*, it is key that the SSU's reform takes into account the different security needs of all, including women, men, girls and boys as well as persons from marginalized communities. This should help shaping more gender- and diversity-responsive security policies that would allow security sector institutions, including the SSU, to more adequately and effectively serves the interests of the State and society as a whole (see par 18 *supra*).
89. Second, security services are part of the public sector, and as such must be held to the same standards as other parts of government, including on gender equality and diversity. This means that security services are bound by national laws concerning non-discrimination and the international legal frameworks prohibiting discrimination and obliging to adopt measures to overcome it.¹²⁰ Accordingly, security services shall not discriminate against individuals or groups on any ground.¹²¹ **It is recommended that the principle of non-discrimination on any ground be expressly stated as a key principle guiding the reform and the activities of SSU, while specifying that it is applicable both to the internal policies and functioning of the SSU as well as its external operational activities.** Indeed, States should ensure that the activities of their security services (in particular in the context of counter-terrorism) are undertaken on the basis of individuals' behaviour, and not on the basis of their national or ethnic origin, colour, language, religion or belief, political or other opinion, social origin, sex, sexual orientation or gender identity, or other status.¹²² Some States have explicitly proscribed their intelligence/security services from establishing files on individuals on this basis,¹²³ which is generally recognized as a good practice.¹²⁴ **Such a clear statement defining and prohibiting such profiling could also be included, either in the Draft Concept or in other relevant legislation.**
90. Third, the SSU's working environment itself should be conducive to more gender equality and diversity. Beyond simply increasing the representation of women, **institutional culture and work practices should be inclusive, non-discriminatory and open to diversity in policy as well as in practice. For instance, this could imply ensuring that work and employment conditions are gender sensitive** (i.e., considering the different ways that men, women and others might struggle to combine work with other responsibilities, such as caring for parents or children)¹²⁵ and that the institution adopts a

¹¹⁸ UN CEDAW Committee, [General Recommendation no. 30 on Women in Conflict Prevention, Conflict and Post-conflict Situations](#), 18 October 2013, par 69.

¹¹⁹ *ibid.*

¹²⁰ *Op. cit.* footnote 25, page 13 (2019 DCAF-OSCE/ODIHR-UN Women Tool no. 14 on Intelligence and Gender). See also ILO, [Discrimination \(Employment and Occupation\) Convention, 1958 \(No. 111\)](#), ratified by Ukraine on 4 August 1961, Article 1 (a), which specifies discrimination as "any distinction, exclusion or preference made on the basis of race, colour, sex, religion, political opinion, national extraction or social origin, which has the effect of nullifying or impairing equality of opportunity or treatment in employment or occupation".

¹²¹ *Op. cit.* footnote 24, Practice 11 (2010 UN SRCT Compilation).

¹²² *ibid.* par 18 (2010 UN SRCT Compilation). See also CERD, [General Recommendation No. 30 on Discrimination Against Non-citizens](#) (2004), par 10.

¹²³ *ibid.* par 18 (2010 UN SRCT Compilation).

¹²⁴ UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, [Report on Racial and Ethnic Profiling](#), A/HRC/29/46, 20 April 2015, par 66. See e.g., CERD, [General Recommendation No. 34 on Racial Discrimination against People of African Descent](#), par 39. In the context of policing, see also ODIHR, [Opinion on the Draft Law of Ukraine on Police and Police Activities](#) (2014), par 30; and Council of Europe's European Commission against Racism and Intolerance (ECRI), [General Policy Recommendation No. 11 on Combating Racism and Racial Discrimination in Policing](#), 29 June 2007.

¹²⁵ *Op. cit.* footnote 25, page 22 (2019 DCAF-OSCE/ODIHR-UN Women Tool no. 1 on SSG/SSR and Gender).

zero-tolerance policy towards harassment, sexual harassment, sexism and various forms of abuse in the working culture of the institution (see par 92 *infra*), among others. There should also be a proper assessment of human resources recruitment, retention, career development, training and promotion policies, processes and materials to ensure that they do not reflect implicit or explicit gender and other biases.¹²⁶ This should then inform a gender equality and diversity strategy to address the cultural and structural obstacles, as well as invisible barriers, preventing recruitment, retention and promotion of women and other underrepresented groups and new recruitment strategies should be shaped to appeal to women and other underrepresented groups.¹²⁷ **These aspects should be expressly reflected in the Draft Concept.**

91. As regards persons with disabilities specifically, Article 27 of the UN Convention on the Rights of Persons with Disabilities (hereinafter “CRPD”)¹²⁸ prescribes their right to work, on an equal basis with others, including the right to gain a living by “*work freely chosen or accepted in a labor market and work environment that is open, inclusive and accessible to persons with disabilities*”. “*Participation on an equal basis*” implies not only that selection and employment criteria must be non-discriminatory, but also that states are obliged to take effective measures to create an enabling environment for the realization of full and equal participation of persons with disabilities, meaning that adequate conditions should be provided to facilitate the work of qualified candidates. **The drafters could consider including a statement to that effect in the Draft Concept.**
92. Moreover, security services must have strong policies and other safeguards, including proper and functioning reporting, complaints and disciplinary mechanisms to prohibit, prevent, detect and respond effectively to human rights violations, including internal and external cases of sexual, gender-based and other types of abuse or harassment, intimidation, exploitation, violence or discrimination based on national or ethnic origin, colour, language, religion or belief, political or other opinion, gender, sexual orientation, gender identity, gender expression or any other ground.¹²⁹ Effective mechanisms must be designed to protect complainants from retaliation by those accused of wrongdoing or by senior staff.¹³⁰ Other safeguards could consist of targeted training and awareness raising programs, mechanisms to ensure accountability of leadership etc. **The Draft Concept should explicitly provide for the development of such policies, safeguards and reporting and complaints mechanisms for both internal and external cases of all types of abuses, harassment, exploitation, violence or discrimination, while ensuring appropriate allocation of human and financial resources for that purpose.**

KEY RECOMMENDATION D.

To provide for strong policies and other safeguards, including proper and functioning reporting, complaints and disciplinary mechanisms to prohibit, prevent, detect and respond effectively to human rights violations, including sexual, gender-based and other types of abuse or harassment, intimidation, exploitation, violence or discrimination based on national or ethnic origin,

¹²⁶ *ibid.*

¹²⁷ *ibid.* page 37 (2019 DCAF-OSCE/ODIHR-UN Women Tool no. 14 on Intelligence and Gender).

¹²⁸ *UN Convention on the Rights of Persons with Disabilities*, adopted by General Assembly resolution 61/106 on 13 December 2006. Ukraine ratified the Convention on 4 February 2010.

¹²⁹ *Op. cit.* footnote 24, Practice 18 (2010 UN SRCT Compilation). *ibid.* page 37 (2019 DCAF-OSCE/ODIHR-UN Women Tool no. 1 on SSG/SSR and Gender); and page 39 (2019 DCAF-OSCE/ODIHR-UN Women Tool no. 14 on Intelligence and Gender).

¹³⁰ For guidance on gender and internal complaints mechanisms, see e.g., DCAF, Megan Bastick, [Gender and Complaints Mechanisms: A Handbook for Armed Forces and Ombuds Institutions to Prevent and Respond to Gender-Related Discrimination, Harassment, Bullying and Abuse](#) (2015). See also OSCE/ODIHR-DCAF-OSCE Gender Section, [Guidance notes on Integrating a Gender Perspective into Internal Oversight within Armed Forces, on Integrating Gender into Internal Police Oversight, and on Integrating Gender into Oversight of the Security Sector by Ombuds Institutions & National Human Rights Institutions](#) (2014).

colour, language, religion or belief, political or other opinion, gender, sexual orientation, gender identity, gender expression or any other ground, while ensuring the protection of whistle-blowers and complainants from retaliation by those accused of wrongdoing or by senior staff. (*see also par 99 infra*)

93. Fourth, this also means that a gender and diversity perspective needs to be integrated at each stage of the full cycle of justice and security provision – analysis, policy-making, design and planning, training, implementation, monitoring and evaluation, management and oversight.¹³¹ This can help improving intelligence gathering and analysis of intelligence by allowing potentially overlooked signs of instability to come to the fore.¹³² **This principle could be explicitly stated in the Draft Concept as a guiding principle of the actions of the SSU.** In terms of institutional and personal capacity of the SSU, the Draft Concept makes a few references to the training of SSU staff but it would be advisable to specify that this should include **gender, diversity and human rights training**.
94. Finally, it is also essential that **gender expertise and the role of women in oversight of the SSU is strengthened**¹³³ (see also Sub-Section 5 *supra* on control and oversight over the SSU). Furthermore, **the participation of women and other under-represented groups in decision-making processes related to SSU’s work (both strategic and operational) as well as in security sector policy and legislative reform processes should also be increased** (see also Sub-Section 8 *infra*).
95. In light of the foregoing, **the Draft Concept should reflect all these aspects and be supplemented to ensure that gender and diversity considerations are mainstreamed throughout the document.**

KEY RECOMMENDATION E.

To enhance the provisions concerning gender, diversity and non-discrimination, including by clearly stating the principle of non-discrimination as one of the key principles guiding the reform and the activities of SSU, and enhancing the provisions concerning and ensuring that gender and diversity are promoted internally as part of the working culture of the institution, as well as externally when delivering security services, and when budgeting and carrying out oversight.

7. HUMAN RESOURCES MANAGEMENT AND FINANCIAL AND LOGISTICAL SUPPORT

7.1. Human Rights and Freedoms of SSU Personnel

96. Nothing is said in the Draft Concept about the human rights and freedoms of SSU personnel, which seems unfortunate. In that respect, the 1994 [OSCE Code of Conduct on Politico-Military Aspects of Security](#) states that “[e]ach participating State will ensure that military, paramilitary and security forces personnel will be able to enjoy and exercise their human rights and fundamental freedoms as reflected in CSCE documents and international law, in conformity with relevant constitutional and legal provisions and with

¹³¹ *Op. cit.* footnote 25, page 21 (2019 DCAF-OSCE/ODIHR-UN Women Tool no. 1 on SSG/SSR and Gender).

¹³² *ibid.* page 9 (2019 DCAF-OSCE/ODIHR-UN Women Tool no. 14 on Intelligence and Gender).

¹³³ UN CEDAW Committee, [General Recommendation no. 30 on Women in Conflict Prevention, Conflict and Post-conflict Situations](#), 18 October 2013, par 69.

the requirements of service".¹³⁴ Restrictions on the human rights and fundamental freedoms of the security personnel may be provided when this is contemplated by international human rights standards and providing that such restrictions are prescribed by law and necessary in a democratic society. **It would be advisable to explicitly recognize the human rights and fundamental freedoms of SSU personnel in the Draft Concept, while ensuring that subsequent legislation will also provide guarantees in that respect.** This also means setting up legal and administrative procedures and mechanisms to protect their rights (see also par 92 *supra* on complaints and disciplinary mechanisms). This is important for good governance in the security sector but also because security officials are more likely to uphold the law and respect human rights and freedom of individuals if their own rights and freedoms are guaranteed and if they are themselves treated with dignity by their superiors, their employers and the public.

97. While a comprehensive overview of the legitimacy and proportionality of potential restrictions to SSU's personnel human rights and fundamental freedoms would go beyond the scope of this Opinion, it is worth emphasizing that **any such restrictions should be strictly necessary and proportionate to ensure the political neutrality and impartiality of the public officials concerned and the proper performance of their duties.**¹³⁵ This principle could also be explicitly mentioned in the Draft Concept.

KEY RECOMMENDATION F.

To explicitly recognize the human rights and fundamental freedoms of SSU personnel in the Draft Concept, while emphasizing that any restriction to their rights and freedoms should be strictly necessary and proportionate to ensure the political neutrality and impartiality of the public officials concerned and the proper performance of their duties.

¹³⁴ See [1994 OSCE Code of Conduct on Politico-Military Aspects of Security](#), par 32.

¹³⁵ See e.g., on the political neutrality of public servants in general, ECtHR, [Ahmed and Others v. United Kingdom](#) (Application no. 22954/93, judgment of 2 September 1998), pars 53 and 63; and [Briške v. Latvia](#) (Application no. 47135/99, decision of 29 June 2000). Article 22.2 of the ICCPR and Article 11.2 of the ECHR allows restrictions to be placed by states on the free association of police and members of the armed forces (and the state administration for the ECHR). See ODIHR-Venice Commission, [Joint Guidelines on Freedom of Association](#) (2014), par 144, where ODIHR and the Venice Commission have specifically acknowledged the possibility of imposing restrictions on the exercise of the right to freedom of association of some public officials in cases "*where forming or joining an association would conflict with the public duties and/or jeopardize the political neutrality of the public officials concerned*". At the same time, a complete ban on forming and joining a trade union would be considered to encroach on the very essence of freedom of association and as such be violating international human rights standards (see e.g., concerning military personnel ECtHR, [Adefdromil v. France](#) (Application no. 32191/09, 2 October 2014), pars 55 and 60; and [Matelly v. France](#) (Application no. 10609/10, 2 October 2014), pars 71 and 75; see also European Committee of Social Rights, [CGIL v. Italy](#), complaint 140/2016, decision of 7 June 2019 on the rights of members of the financial guards, who have military status, to establish and join trade unions (Article 5), to negotiate collective agreements (Article 6§2) and to strike (Article 6§4 - the decision confirming the necessity and proportionality requirement). As to political activities and membership in a political party, the [OSCE/ODIHR-Venice Commission Guidelines on Political Party Regulation](#) (2011) specifies that "*partisan political participation and party membership of public officials may be regulated or denied in order to ensure that such persons are able to fulfil their public functions free of a conflict of interest*" (par 117). On the political passive (standing up for election) and active (right to vote) aspects of political participation of military personnel, see also ECtHR, [Etxeberria and Others v. Spain](#) (Application nos. 35579/03, 35613/03, 35626/03 and 35634/03, judgment of 30 June 2009), par 50; [Davydov and Others v. Russia](#) (Application no. 75947/11, judgment of 30 May 2017), par 286; [Ždanoka v. Latvia](#) [GC] (Application no. 58278/00, judgment of 16 March 2006), par 115; and [Melitchenko v. Ukraine](#) (Application no. 17707/02, judgment of 19 October 2004), par 57. As to the right to freedom of religion or belief, it may be legitimate for a state to impose on civil servants, on account of their status, a duty to refrain from any ostentation in the expression of their religions or beliefs in public (see e.g., ECtHR, [Pitkevich v. Russia](#) (Application no. 47936/99, decision of 8 February 2001). As such, limiting the manifestation of religion or belief during the exercise of their public functions and in other situations that are linked to one's work may be justifiable given the need for neutrality and impartiality; however, this should not be interpreted as limiting their right to manifest their religions or beliefs outside of work, in worship, teaching, practice and observance, under Article 18 of the ICCPR, so long as this does not question their neutrality and impartiality. As to freedom of expression, any individual's right to freedom of expression may be limited, as outlined in Article 19(3) of the ICCPR, if such restrictions are provided by law, are necessary out of respect of the rights or reputations of others, or in order to protect national security, public order (*ordre public*), or public health or morals, and are proportionate to such aims. Legitimate restrictions of public servants primarily derive from the principle of confidentiality, binding them to professional secrecy with regard to information obtained in the course of their functions and to the need to maintain the neutrality of the service.

7.2. Human Resources Management

98. Section 6 of the Draft Concept, which concerns SSU's human resources management system, is silent as to the ethical and disciplinary rules applicable to the SSU personnel. It would be advisable **to include a paragraph on the development and implementation of code of ethics / code of conduct in line with international standards, which should serve as an additional guidance for internal control.**
99. **It would also be important to include in the Draft Concept a specific reference to the protection of “whistleblowers”** (i.e., individuals releasing confidential or secret information although they are under an official or other obligation to maintain confidentiality or secrecy) **against legal, administrative or employment-related sanctions if they act in “good faith” when releasing information.**¹³⁶ Indeed, given that the great majority of SSU's work is naturally clandestine, most of the time persons whose rights are violated (for instance through unlawful surveillance) are not aware of such violations, and cannot seek remedy. The oversight institutions are only as powerful as their mandates and their access to information allow for. In democratic societies, accountability and oversight mechanisms are complemented with well-regulated whistleblowing procedures, allowing staff of security/intelligence agencies to raise concerns and report to competent internal and external authorities (and in extreme cases to the public) about suspected/witnessed misconduct and violations, including human rights violations.¹³⁷ In 2015, PACE adopted the *Resolution (2060)* recalling previous Resolutions endorsing the Tshwane Principles, and calling on Member States to “*enact whistle-blower protection laws also covering employees of national security or intelligence services and of private firms working in this field*”.¹³⁸ For instance, in France, staff of the intelligence services who witness or observe violations of the intelligence law can address the National Commission for Monitoring of Intelligence Techniques (CNCTR), which can then bring the case before the Council of State and inform the Prime Minister.¹³⁹

7.3. Financial and Logistical Support

100. The 1994 *OSCE Code of Conduct on Politico-Military Aspects of Security* stipulates that “[e]ach participating State will provide for its legislative approval of defence expenditures” and “will, with due regard to national security requirements, exercise restraint in its military expenditures and provide for transparency and public access to information related to the armed forces” (par 22). It is generally assumed that the participating States of the CSCE wanted these principles to apply not only to defence expenditures, but also to other security-related spending. In Ukraine, the expenditures of the SSU are approved by the legislature (Section 8.1 of the Draft Concept), which is in conformity with the *1994 OSCE Code of Conduct*. However, some questions arise regarding the transparency of the budget process and public access to such information and the rigour of budgetary control. It is not clear how detailed the budget submitted to the Verkhovna Rada is and whether it specifies the activities of the SSU. **It is recommended to include in the Draft Concept a provision on improving the transparency of the budget process of the SSU, in the spirit of paragraph 22 of the 1994 OSCE Code of Conduct.**
101. Another critical stage in the budget process is the monitoring of government agencies' expenditures. In that respect, the Draft Concept specifies that the “*external financial*

¹³⁶ *ibid.* Sub-Section on “Secrecy Legislation”, 4th paragraph (2004 Joint Declaration).

¹³⁷ See e.g., *op. cit.* footnote 24, Principles 37-49 (Tshwane Principles).

¹³⁸ *Op. cit.* footnote 24, Article 10.1.1 (2015 PACE, [Resolution 2060 on improving the Protection of Whistle-blowers](#)).

¹³⁹ *Op. cit.* footnote 24, page 31 (2017 EU FRA Surveillance by Intelligence Services). See also e.g., France, Interior Security Code, Article L. 861-3.

control (audit) over the activity of the Security Service of Ukraine shall be carried out by the Accounting Chamber” (Section 8.1), which is in line with OSCE commitments and good practices. However, if the Accounting Chamber is to be able carry out such functions in relation to the SSU, it will need an adequate apparatus of its own as well as detailed information on the budget of the SSU. It will also need full access to the SSU’s accounting books, which should provide a clear picture of how the allocated funds have been spent. In practice, this has sometimes proved to be a challenge in certain countries.¹⁴⁰ Hence, and while it is welcome that the internal control and audit system at the SSU is to be “optimized” (Section 3.2. of the Draft Concept), **it is recommended to add that the SSU’s accounts should be made more accessible for audit by the Accounting Chamber and other bodies responsible for the external audit of the SSU, including the relevant parliamentary committee** (see par 77 *supra*).

102. Finally, achieving greater gender balance and representation within the SSU and ensuring that gender and diversity considerations are an integral part of all the dimensions of SSU’s functioning and work will also require thorough assessment of the impact of its institutional budgetary allocations and expenditures.¹⁴¹ For example, separate financial allocations may need to be made to enhance organizational gender expertise, including through creation of new positions, establishment of measures to address gender-based discrimination and harassment, as well as possible individual circumstances (e.g., maternity and parental leave). **It is recommended to include in the Draft Concept a provision on incorporation of gender perspective in SSU’s budget process.**

8. FINAL COMMENTS ON THE PROCESS OF PREPARING AND ADOPTING THE DRAFT CONCEPT AND RELATED LEGISLATION

103. As mentioned in Sub-Section 2.1 *supra*, it is key that security policy and legislation are developed taking into consideration security needs that are defined in an inclusive, gender-responsive manner,¹⁴² ensuring that communities and individuals participate in articulating their own security needs. Especially, the [UN Security Council Resolution 1325 “Women, Peace and Security”](#) (2000) encourages the equal participation and full involvement of women in all efforts for the maintenance of peace and security and urges states to increase the participation of women in all UN peace and security efforts, including decision-making related to security.¹⁴³ OSCE [Decision No. 7/09 on Women’s Participation in Political and Public Life](#) also calls upon OSCE participating States to introduce where necessary open and participatory processes that enhance participation of women and men in all phases of developing legislation, programmes and policies (par 5).
104. It is indeed important to seek a broad-based national vision on security sector reform, informed by the needs and aspirations of the population. In defining this vision, states should apply a holistic, participatory and transparent approach to security sector reform, based on an inclusive dialogue process among and between authorities at various levels, from all branches of government and security sector institutions, national human rights institutions, civil society,¹⁴⁴ especially women’s groups and child protection advocates, representatives from marginalized communities or groups, religious and belief

¹⁴⁰ In the Netherlands, for instance, the defence expert of the supreme audit authority complained about 10 years ago that the Ministry of Defence was trying to be transparent but was nonetheless difficult to audit because its bookkeeping was not clear enough.

¹⁴¹ See e.g., *op. cit.* footnote 25, Sections 33, 4.3 and 5.1 (2019 DCAF-OSCE/ODIHR-UN Women Tool no. 7 on Parliamentary Oversight of the Security Sector and Gender).

¹⁴² *Op. cit.* footnote 25, (2019 DCAF-OSCE/ODIHR-UN Women Tool no. 1 on SSG/SSR and Gender).

¹⁴³ [UN Security Council Resolution 1325 “Women, Peace and Security”](#) (2000), par 1. See also *op. cit.* footnote 25, page 11 (2019 DCAF-OSCE/ODIHR-UN Women Tool no. 1 on SSG/SSR and Gender).

¹⁴⁴ OSCE participating States have committed to the aim of “strengthening modalities for contact and exchanges of views between NGOs and relevant national authorities and governmental institutions” (Moscow 1991, para. 43.1).

communities, and other non-State actors.¹⁴⁵ This will help increasing local acceptance of security actors, as well as giving them important insights as to how to improve in fulfilling their tasks.¹⁴⁶ This is especially important since, in a recent mapping of security sector assistance programmes in Ukraine, the issue of lack of involvement of media and CSOs in policy developments and implementation of security sector-related reform was emphasized.¹⁴⁷ The OSCE has specifically noted that one of the main problems is that the CSOs' efforts to participate in reforms are often ignored by public institutions on the central and regional levels alike.¹⁴⁸

105. Accordingly, **the Draft Concept should be developed and adopted through a broad, inclusive and participatory process and therefore include the above-mentioned stakeholders, including CSOs, in a timely fashion in public discussions on the Draft Concept.** This means that the public, including women and men, and a wide array of associations representative of various views, even those that are critical of the government/state, should be consulted in the conceptualization and implementation of the Draft Concept.¹⁴⁹ An important part of intelligence reform involves actively questioning how intelligence services should be defined in a democratic society and this can only be done through meaningful participation of civil society, academia and media platforms¹⁵⁰
106. The same comment should apply to any legislation adopted pursuant to the Concept, especially the contemplated amendments to the Law of Ukraine on the Security Service of Ukraine (Section 3.2, 1st indent).¹⁵¹ Indeed, OSCE participating States have committed to ensure that legislation will be “*adopted at the end of a public procedure, and [that] regulations will be published, that being the condition for their applicability*” (1990 Copenhagen Document, par 5.8).¹⁵² Moreover, key OSCE commitments specify that “[l]egislation will be formulated and adopted as the result of an open process reflecting the will of the people, either directly or through their elected representatives” (1991 Moscow Document, par 18.1).¹⁵³ As such, public consultations constitute a means of open and democratic governance as they lead to higher transparency and accountability of public institutions, and help ensure that potential controversies are identified before a law is adopted.¹⁵⁴ Consultations on draft legislation and policies, in order to be effective, need to be inclusive and to provide relevant stakeholders with sufficient time to prepare and submit recommendations on draft legislation.¹⁵⁵ Moreover, given the potential impact of the reform, it is essential that such reform be preceded by an in-depth research and impact assessment, completed with a proper problem analysis using evidence-based techniques to identify the best efficient and effective regulatory option.¹⁵⁶ It is also key that proper time be allocated for the preparation and adoption of amendments.
107. In that respect, the logical sequencing is to first carry out a proper regulatory impact assessment and then develop policy document to frame the general orientations of the reform. This should subsequently guide the development of national security legislation

¹⁴⁵ *Op. cit.* footnote 26, par 61(a) (2013 UN Secretary-General's [Report on Securing States and Societies](#)).

¹⁴⁶ *Op. cit.* footnote 25, page 27 (2019 DCAF-OSCE/ODIHR-UN Women Tool no. 1 on SSG/SSR and Gender).

¹⁴⁷ See DCAF, [Supporting Ukraine's Security Sector Reform – Mapping Security Sector Assistance Programmes](#) (2018), page 56.

¹⁴⁸ See OSCE Special Monitoring Mission to Ukraine, [Civil Society and the Crisis in Ukraine](#), SEC.FR/125/15/Corr.1, 11 February 2015, page 10.

¹⁴⁹ See Vienna Recommendations on Enhancing the Participation of Associations in Public Decision-Making Processes (April 2015), available at <<http://www.osce.org/odihr/183991>>.

¹⁵⁰ *Op. cit.* footnote 25, page 30 (2019 DCAF-OSCE/ODIHR-UN Women Tool no. 14 on Intelligence and Gender).

¹⁵¹ See par 18.1 of the [OSCE Document of the Moscow Meeting](#) (1991).

¹⁵² Available at <<http://www.osce.org/fr/odihr/elections/14304>><http://www.osce.org/fr/odihr/elections/14304>>.

¹⁵³ Available at <<http://www.osce.org/fr/odihr/elections/14310>><http://www.osce.org/fr/odihr/elections/14310>>.

¹⁵⁴ *ibid.*

¹⁵⁵ According to recommendations issued by international and regional bodies and good practices within the OSCE area, public consultations generally last from a minimum of 15 days to two or three months, although this should be extended as necessary, taking into account, *inter alia*, the nature, complexity and size of the proposed draft act and supporting data/information. See e.g., ODIHR, [Opinion on the Draft Law of Ukraine “On Public Consultations”](#) (1 September 2016), pars 40-41.

¹⁵⁶ See e.g., ODIHR, [Report on the Assessment of the Legislative Process in the Republic of Moldova](#) (2010), par 14.5.

and other programmes on the basis of such policy documents. In that respect, the fact that the Bill no. 3196 on amending the *Law of Ukraine “On the Security Service of Ukraine”* was registered with the Verkhovna Rada on 12 March, even before the adoption of the Concept may appear premature.

108. Accordingly, the process by which future amendments will be developed and adopted in accordance with the Draft Concept should conform with principles of democratic law-making. Any legitimate reform process relating to the security sector, especially of this scope, **should be transparent, inclusive, extensive and involve effective consultations, including with representatives of civil society organizations and a full impact assessment including of compatibility with relevant international human rights standards. Adequate time should also be allowed for all stages of the preparation of the amendments and ensuing law-making process.** ODIHR remains at the disposal of the authorities for any further assistance that they may require in any legal reform initiatives pertaining to the security sector or in other fields.

[END OF TEXT]
