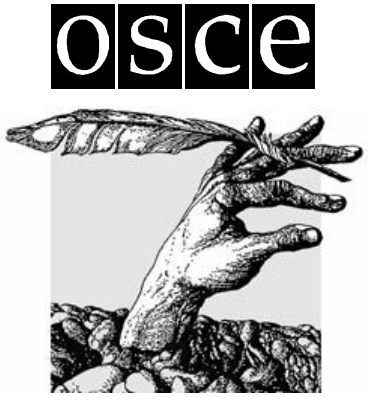

The Representative on Freedom of the Media

Comments on the Law on Protection of State Secrets of the Kyrgyz Republic[1]

David Banisar
Director, Freedom of Information Project of Privacy International[2]
September 2005

Introduction

The Law on Protection of State Secrets is a significant barrier to the right of freedom of information of the media and people of the Kyrgyz Republic. The government should take the opportunity while it is considering the Draft Law on the Freedom and Guarantees of Access to Information to rescind this obsolete law and replace it with one that is forward looking and democratic that recognizes the importance of access to information.

The new law should work hand in hand with new legislation on access to information to ensure maximum access to information while providing protection to that information essential for national security. The government should also begin a process of declassification of records from the previous government.

The Costs of Secrecy

The most important consequence of excessive secrecy is that it undermines public trust in government, especially when used in abusive ways such as to support political agendas or hide abuses, corruption and mismanagement. If the public only believes that the government is doing something for its own benefit because excessive secrecy has led the public to be uninformed or misinformed about government activities, the credibility and legitimacy of that

[1] This analysis is based on translations of the draft law on information provided to the author in August 2005.
[2] Homepage: http://www.privacyinternational.org/foi

government is seriously undermined and it will have grave difficulties in gaining public support for any of its activities.

There are other direct damages from excessive secrecy. Excessive classification can lead to a weakening of the protections of important information. Even the most secret of files can be leaked when the classification system is not carefully organized. As US Supreme Court Justice Potter Stewart noted in the *Pentagon Papers* case in 1971, "when everything is classified, then nothing is classified, and the system becomes one to be disregarded by the cynical or the careless, and to be manipulated by those intent on self protection or self-promotion."[3] In Hungary, the former secret police file of Prime Minister Peter Medgyessy was leaked in 2002 revealing that he had once worked for a branch of the intelligence services. In February 2005, a list of 240,000 names of agents, informers, and victims of the Polish Communist-era secret police was leaked and placed on the Internet.

It also prevents the learning of important information and lessons. In China, secrecy over the emergence of the SARS virus led to its spread worldwide. The effects are still being felt as new avian flu viruses have emerged and there is little knowledge on how to prevent more outbreaks as the government continues to deny information. The effects are also felt inside governments. The September 11 Commission in the United States found many examples of excessive classification preventing information sharing between government bodies.[4]

There are also direct monetary costs. The creation and protection of classified information imposes significant burdens on public authorities. They must conduct background checks, provide education and training, and provide for physical and electronic security. In the US, the estimated cost of creating and protecting classified information was $7.2 billion in 2004, not including the CIA.[5] Another $1 billion was spent by private businesses under contract to government bodies.

The Relationship between Freedom of Information and the Protection of State Secrets

Every nation rightly sets the protection of national security as a key priority. Thus, most countries have adopted some form of regulations for the protection of information of key importance to national security. At the same time, it is now widely recognized that it is equally essential for governments to make information available to citizens. Access to information facilitates public knowledge and discussion. It provides an important guard against abuses, mismanagement and corruption.

To be effective, limitations on access for national security reasons must be limited in scope, reasonable, and balanced with the need for public access to information in a free and democratic society. A properly functioning security of information system recognizes that a

[3] NY Times v. US, 403 US 713 (1971) . For more details, see National Security Archive, The Pentagon Papers Case. http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB48/

[4] National Commission on Terrorist Attacks Upon the United States, Final Report. http://www.9-11commission.gov/report/index.htm

[5] Information Security Oversight Office, 2004 Report on Cost Estimates for Security Classification Activities, May 2005. http://www.archives.gov/isoo/reports/2004-cost-report.html

limited amount of sensitive information needs to be protected and then only for the duration that it is sensitive. Less sensitive information is given lesser protections or none at all.

The best approach is to set the FOI law as a primary law and ensure that it contains adequate protections for sensitive national security information. If a secrets act is necessary to set procedures for classification and vetting, any decision made under it should not be considered conclusive and all requests for information that has been classified as a state secret are subject to a review of the harms and public interests in the release of the information.

This approach has been adopted in a number of jurisdictions. The New Zealand Official Information Act repealed the 1951 Official Secrets Act. Procedures for classification are detailed in a Cabinet document but all decisions are made under the OIA. Similar procedures are in place in the UK and Canada where the OSA remains in force. In India, the Right to Information Act overrides the Official Secrets Act, 1923. In Mexico, the Federal Law of Transparency and Access to Public Government Information sets the standards for classification and the Federal Commission on Access to Information is the ultimate arbiter of whether something is properly classified or not.

Comments on the Law on Protection of State Secrets

Overly Broad Scope of the Definition of State Secrets

The most significant problem with the law is its broad scope. The definitions are so indefinite that there are few limits and widely discretionary powers are given to officials. It also applies to areas largely unrelated to essential national security interests.

"State secrets" is defined in Article 1 as “information stored and transferred on any media which affects the Kyrgyz Republic’s defence capacity, security, economic and political interests”. Article 5 sets out three categories of state secrets: state, military and official secrets. State secrets are defined as, “information whose disclosure may entail grave consequences for defence capacity, security and economic and political interests of the Kyrgyz Republic.” Military secrets are defined as “military information whose disclosure may cause damage to the Armed Forces and prejudice the interests of the Kyrgyz Republic.” Official secrets is a catch all category covering “information whose disclosure may adversely affect the Kyrgyz Republic’s defence capacity, security and economic and political interests. Such information consists of isolated data that are part of state or military secrets, but do not reveal them in full.”

The use of broad classification categories in state secrets acts is considered by the UN Human Rights Committee to be a violation of Article 19 of the International Covenant of Civil and Political Rights. Their evaluation of the Uzbek Law on Protection of State Secrets (which is similar to the Kyrgyz) stated:

> The Committee is particularly concerned about the definition of "State secrets and other secrets" as defined in the Law on the Protection of State Secrets. It observes that the definition includes issues relating, inter alia, to science, banking and the commercial sector and is concerned that these restrictions on the freedom to receive and impart information are too wide to be consistent with article 19 of the Covenant…The State party should amend the Law on the Protection of State Secrets

> to define and considerably reduce the types of issues that are defined as "State secrets and other secrets", thereby, bringing this law into compliance with article 19 of the Covenant.[6]

This is further compounded by the discretionary powers given to the government and the heads of bodies to define state secrets. Article 14 of the law authorizes the government to draft and approve a "List of Critical Information Items Constituting a State Secret" and approve the "Lists of Information Items Subject to Classification" developed by the heads of government bodies. The practice of creating lists in this manner in Russia was strongly criticized by the Parliamentary Assembly of the Council of Europe in 2003 when it was used against journalists and environmental protection groups:

> The Assembly finds that the most important conclusion to be drawn from Mr Pasko's case is that the definition of what constitutes a state secret must be clarified and, first and foremost, made public. It is unacceptable that whilst the (public) Federal Law on State Secrets contains some three dozen broadly drafted items, their detailed wording is contained in a secret decree by the Minister of Defence (Decree No. 55:96) which mentions some 700 instances of such secrets. This gives the security services wide latitude in prosecuting treason cases, thus providing a formidable instrument of intimidation against courageous journalists such as Mr Pasko and researchers such as Mr Nikitin, who was finally acquitted in September 2000 after having been prosecuted for more than four years on the basis of Decree No. 55:96. The Assembly therefore calls on its colleagues in the Russian State Duma to initiate a law ensuring that secret decrees containing elements of penal law can never again become the basis for criminal convictions.[7]

The better approach would be for the law to set out limited categories of information to be protected that are only related to national security. For example, the US Executive Order on Classified National Security Information sets out eight areas that are eligible for classification:

> (a) military plans, weapons systems, or operations;
> (b) foreign government information;
> (c) intelligence activities (including special activities), intelligence sources or methods, or cryptology;
> (d) foreign relations or foreign activities of the United States, including confidential sources;
> (e) scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism;
> (f) United States Government programs for safeguarding nuclear materials or facilities;
> (g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism; or
> (h) weapons of mass destruction.[8]

[6] Concluding observations of the Human Rights Committee : Uzbekistan. 26/04/2001. CCPR/CO/71/UZB
[7] Resolution 1354 (2003), Conviction of Grigory Pasko.
[8] Executive Order 13,292 on Classified National Security Information, March 28, 2003.

To be eligible for classification, the person making the determination first, "determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, which includes defense against transnational terrorism, and the original classification authority is able to identify or describe the damage."

In Estonia, the State Secrets Act sets out specifically each of the types of information that can be classified, under which category they can be classified, and for how long they can be classified.[9] In Sweden, all exemptions to the Freedom of the Press Act are specifically adopted by Parliament as amendments to the Act on Secrecy.[10] Nothing else can be classified and withheld from the public.

Coverage of Non State Secrets

The law also imposes restrictions on information in an even broader category than state secrets. Article 6 of the law sets obligations for "non state secrets" which are defined as "business secrets, information for official use only, off-the-record information, (criminal) investigation secrets, medical secrets, personal and other secrets." There is a duty imposed on the owners and those who received them in connection with their duties or professional activities to keep them confidential. The rules on protection are set by other laws or by the owners.

This article is clearly out of place in a law otherwise about protection of "state secrets" and should be eliminated. It is unclear why it is even necessary to have in the first place. If these other areas are already protected by other laws, then this section is redundant. If they are not protected, then including them in a law on state secrets would appear to greatly expand the coverage of the law and impose strict penalties designed to protect national security on areas outside the scope of the law. New legislation should be adopted for those areas such as personal information and business secrets, if necessary.

Tiers of State Secrets Undefined

Article 5 sets up three tiers of state secrets: Extremely Sensitive, Top Secret and Secret. State Secrets can be classified as either Top Secret or Secret, Military Secrets can be classified as Top Secret and Secret and Official Secrets can be classified as Secret. This is consistent with international practices and is necessary to ensure that information that is more sensitive is better protected than less sensitive information.

However, the law fails to provide any additional guidance or limits on how the categories are to be applied. While other countries set standards for classification in their laws, the Kyrgyz law only generally states that the procedure is to be determined by the government.

A better approach adopted in many other nations gives more detail on the levels of harm that much be reached for each of the categories. The Polish Classified Information Protection Act sets strong criteria for its two levels of state secrets:

[9] State Secrets Act. RT I 1999, 16, 271 §§ 4-8.
[10] Act on Secrecy of March 20, 1980 as amended.

"top secret"--where an unauthorised disclosure thereof might cause a grave threat to the independence of the Republic of Poland (or to) the inviolability of its territory or its international relations, or carry a threat of irreversible or heavy injuries to national defence interests, to the security of the state and citizens or to other important state interests, or expose those interests to great danger;

"secret"--where an unauthorised disclosure thereof might cause a threat to the international position of the state, to national defence interests, security interests of the state and citizens, or other important interests of the state, or expose those interests to a substantial damage.[11]

The US Executive Order requires "exceptionally grave damage to the national security" for a "Top Secret" classification and "serious damage" for a "Secret" classification. In addition, the person or organisation that issues the classification must also "identify or describe" the threat to allow for more informed review of the order by higher authorities.

Indefinite Duration of Secrets

Another significant flaw in the law is the absence of fixed limits on the duration that information can be classified. Article 9 states that "Classified information shall be de-classified within the time frame set at the time of the classification thereof, unless the decision to extend the classification period is made in accordance with the established procedure."

This procedure is significantly weaker than is found in laws even in other CIS countries. Most secrets laws recognize that a maximum time frame should be set for each category of classification otherwise the information will likely never be declassified. Instead, this is left to the discretion of the government as the issuer of the regulations on applying the law and can be changed at any time.

The current international practice is to set a general limit on the maximum duration of classified information to between fifteen and twenty years for the most sensitive category and progressively less for the lower categories. In Georgia, the Law on State Secrets sets the duration for information categorized as "Of Extraordinary Importance" at twenty years, Top Secret for ten years, and Secret information can only be withheld for five years.[12] The Law on Protection of State Secrets of the Republic of Kazakhstan defines as state secrets as having a limit of twenty years unless there are urgent reasons such as defensive capability.

In the US, the Executive Order on Classification sets a default for information to be classified for ten years unless the person who issues the classification can identify an earlier date or event that would cause it to be available earlier or makes a specific determination that it is sensitive to near a later date. Since its adoption, fifty percent of all information is set for declassification in 10 years or less.[13]

[11] Classified Information Protection Act of 22 January 1999.
[12] Law of Georgia on State Secrets, No. 455-Is, 29 October 1996.
[13] Information Security Oversight Office, Annual Report 2003.

Another important provision missing from the law is the requirement for periodic review of information once is it classified to ensure that it does not remain classified once the reason for its status has expired. The law sets no requirements for periodic review of the categories set by government bodies or of the information itself. The Estonia State Secrets Act requires that each possessor of secrets review the classification yearly and note when it has been declassified. In Sweden, the classification is reevaluated each time the document is accessed.

Limits on Categories of Information Prohibited from Being Designated as State Secrets

Article 4 of the Law sets out five categories of information that cannot be classified as a state secret. These relate to: natural disasters and emergencies; catastrophes and their consequences, the state of the environment, natural resources, public health care, sanitation conditions, culture, agriculture, education, retail trade, and law enforcement; illegal actions by officials and public authorities; and actions that violate citizens' rights and lawful interests and endanger people's security.

This approach is common in both CIS and CEE countries laws on classification and forms an important barrier to the misclassification of information that it is in the public interest to be public. Some areas such as environmental protection are required by the UNECE Convention on Access to Information, Public Participation in Decision-making and Access to Justice in Environmental Matters. Others are required by UN treaties on human rights.[14] However, the categories in the law are fairly minimal and do not apply to many important areas. The following are additional areas found in other laws that should also be set out in the new law:

- *Inefficiency, errors and embarrassment.* The Moldovan and Kazakh laws prohibit the classification of information about the inactivity of public authorities and officials. Under the Romanian Law on Protection of Information, information cannot be made a state secret to hide "administrative errors, limitation of access to information of public interest, illegal restriction of exercising the rights of any person or harming other legitimate interests."[15] The US Executive Order prohibits the classification of information to "prevent embarrassment to a person, organization or agency, retain competition, or prevent or delay the release of information that does not require protection in the interest of national security information."

- *Basic scientific information*. The Romanian Law on Protection of Information and the US Executive Order prohibit the classification of basic scientific information with no connection to national security.

- *Basic statistics and information.* The Lithuanian Law on State Secrets prohibits the classification of "statistical data concerning the state of economy and finances, except for the information which is provided for in the list of state secrets, as well as the state of health care, education, ecology, social and demographic situation, [and] results of

[14] The UN Working Group on Arbitrary Detention, Recommendation: Human Rights and State Secrets, E/CN.4/2001/14, 20 December 2000.
[15] Law no. 182 of April 12th, 2002 on the protection of classified information. Published in the Official Gazette, Part I no. 248 of April 12th 2002.

social studies." The Law of Georgia On State Secrets prohibits the classification of non-military maps.

- *Health of leaders.* The Russian Federation Law on State Secrets and the Georgian law prohibit the classification of information about the health of top officials.

- *Benefits and compensation.* The CIS Interparliamentary Assembly Model Law, the Russian Federation and the Georgian law on State Secrets all prohibit classification of information about the "privileges, compensations and benefits granted by the State to individuals, officials, and also to enterprises, institutions, and organizations." [16]

- *Natural resources and currency reserves*. The Russian Federation law prohibits classification about gold reserves and recently President Putin declassified information relating to diamonds and platinum.

- *International agreements and acts.* The Georgian law prohibits the classification of international agreements and treaties and most normative acts.

Protecting Whistleblowers and Public Interest Releases

The law should also provide an exemption for the unauthorized disclosure of classified information when there is a strong public interest in its disclosure. The UN Human Rights Committee has been critical of states that use secrets acts to repress important information. In 2001, it criticized the United Kingdom government for using the Official Secrets Act against whistleblowers and journalists:

> The Committee is concerned that powers under the Official Secrets Act 1989 have been exercised to frustrate former employees of the Crown from bringing into the public domain issues of genuine public concern, and to prevent journalists from publishing such matters.
>
> The State Party should ensure that its powers to protect information genuinely related to matters of national security are narrowly utilised, and limited to instances where it has been shown to be necessary to suppress release of the information.[17]

A number of the agreements that the Kyrgyz Republic has agreed to in the field of anti-corruption call on countries to adopt protections for whistleblowers who reveal corruption. Pillar 3 of the Asian Development Bank/Organisation for Economic Cooperation and Development Anti-Corruption Action Plan for Asia and the Pacific, which the Kyrgyz Republic formally endorsed in November 2003, calls on governments to adopt whistleblower protections for both public and private sectors employees who reveal corruption.[18] Pillar 2 of the Istanbul Anti-Corruption Action Plan that the Kyrgyz Republic joined in November 2003

[16] Model Law On State Secrets. Adopted at the twenty-first plenary session of the CIS Interparliamentary Assembly (decision № 21-10 of 16 June 2003).
[17] Concluding Observations of the Human Rights Committee : United Kingdom of Great Britain and Northern Ireland. 05/11/2001. CCPR/CO/73/UK,CCPR/CO/73/UKOT.
[18] ADB OECD Anti-Corruption Initiative, Anti-Corruption Action Plan for Asia and the Pacific. http://www1.oecd.org/daf/asiacom/ActionPlan.htm

also calls for the protection of whistleblowers. In addition, the Council of Europe Civil Law Convention on Corruption also recognizes that employees who disclose information about corruption should not be subject to sanctions.[19]

Classifying Private Information

Article 8 of the law allows for designated government at their own initiative to classify or declassify as state secrets information in the possession of legal entities and citizens. Losses are reimbursed to the owner who can appeal the decision to a court.

This provision is extremely problematic. It allows government agencies to classify information that it did not generate or possess. Similar provisions are typically found in CIS countries but not in any countries in western or central Europe. Experience has shown that these provisions are often abused, especially against media and independent researchers who are revealing information critical of government bodies.[20] As noted above, the Parliamentary Assembly of the Council of Europe has been very critical of the use of the powers of government bodies to determine on their own what is to be classified or not and then impose it against non-officials. The UN Working Group on Arbitrary Detention has also recommended that states refrain from classifying information held by civil society groups in ways that abuse the Article 19 rights of the persons.[21]

Oversight

Under Article 16, the Ministry of Justice is assigned broad powers for "coordinating, advisory and supervisory functions to protect state, military or official secrets from public disclosure in the press." The Kyrgyz Republic State Committee for National Security and the information security units of ministries, state committees, administrative departments, enterprises, institutions and organizations are also given undefined authority.

There is a growing recognition that the most effective means to ensure a balanced classification policy is to appoint an independent body to develop policy, review decisions and monitor developments. In the United States, the Information Security Oversight Office, a division of the National Archives, has extensive powers including: implementing directives, instructions and regulations; inspections and general oversight; security education and training; receiving and taking action on complaints, appeals, and suggestions from persons inside or outside the executive branch; statistical collection, analysis and reporting; acting as a spokesperson for government security policy; conducting special studies and projects; recommending policy changes to the President; and convening and chairing interagency meetings to discuss matters.

In Bulgaria, the Law for the Protection of Classified Information created the State Commission for the Security of Information (SCSI), a new state body responsible to the

[19] Council of Europe, Civil Law Convention on Corruption, ETS No 174. http://conventions.coe.int/treaty/en/Treaties/Html/174.htm

[20] See Bellona, The Nikitin Case. http://www.bellona.no/imaker?id=15049&sub=1

[21] OPINION No. 19/1999 (CHINA). E/CN.4/2000/4 /Add.1, 17 December 1999; OPINION No. 9/1999 (RUSSIAN FEDERATION), E/CN.4/2000/4 /Add.1,17 December 1999; Recommendation: Human Rights and State Secrets, E/CN.4/2001/14, 20 December 2000.

Council of Ministers and National Assembly.[22] The SCSI has been given extensive powers over control of classified information. In Hungary, under the Secrecy Act of 1995, the Parliamentary Commissioner for Data Protection and Freedom of Information is entitled to change the classification of state secrets.[23]

Other countries have created specialized commissions for certain information or purposes. In France, a 1998 law on classification of national security information[24] created the Commission consultative du secret de la défense nationale (CCSDN), which gives advice on the declassification and release of national security information in court cases. The advice is published in the Official Journal.[25] In many CEE countries, specialized bodies have been created to oversee the processing and eventual release of information relating to the archives of the former secret police. In Germany, since 1991, the German Federal Commission for the Records of the State Security Services of the Former GDR (the Gauck Authority) has a staff of 3,000 piecing together shredded documents and making files available.[26] In Romania, the 1999 Law on the Access to the Personal File and the Disclosure of the Securitate as a Political Police created the National Council for the Search of Security Archives (CNSAS) to oversee the archives of the Securitate and facilitate Romanian citizens' access to their Securitate files. It also allows public access to the files of those aspiring for public office and other information relating to the activities of the Securitate.[27]

Breaking with the Past – Bulk Declassification of Older Documents

The recent dramatic changes in government also present a unique opportunity for Kyrgyzstan to make a clear break with the past by declassifying the documents of previous governments. This has been done in many CEE countries when transitioning to new governments. In Bulgaria, the Prime Minister by executive order in 1994 decreed that the secret police files of the communist-era were to be all declassified. In Poland, the Classified Information Protection Act required that all pre-1990 records be reviewed and those found to be not necessary to continue to keep secret were automatically released within 36 months. In Hungary, the Act on State and Official Secrets required the review and declassification of all records from before 1980 within one year of its enactment.

It should be obvious that nearly all the records of the previous government will have little sensitivity in a democratic system and should be made public. They were classified under a system that often arbitrarily kept information secret to protect its political power and with little interest in the needs of the citizens of Kyrgyzstan. The release of these documents will

[22] Law for the Protection of the Classified Information. Prom. SG. 45/30 Apr 2002, corr. SG. 5/17 Jan 2003
[23] Hungary, Act LXV of 1995 on State Secrets and Official Secrets.
[24] Loi no 98-567 du 8 juillet 1998 instituant une Commission consultative du secret de la défense nationale, http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=DEFX9700140L See Rapport 2001 de la Commission consultative du secret de la défense nationale, http://www.ladocumentationfrancaise.fr/brp/notices/014000754.shtml
[25] For a copy of decisions, see http://www.reseauvoltaire.net/rubrique387.html
[26] Web Site: http://www.bstu.de/home.htm
[27] Homepage: http://www.cnsas.ro/indexeng.html. Law No. 189/7 December 1999 on the access to the personal file and the disclosure of the Securitate as a political police, http://www.cnsas.ro/legeng.htm. See Ioana Borza, Decommunization in Romania: A Case Study of the State Security Files Access Law http://www.polito.ubbcluj.ro/EAST/East6/borza.htm

free up valuable resources that are currently being used for their protection and allow government authorities to just focus on keeping important information safe.

This is especially important for the release of records of the intelligence services. Following the transition to democracy, most Central and Eastern European countries adopted laws to address the files of the former secret police forces. These files are made available to individuals to see what is being held on them.[28] The most advanced law on access is in Germany. Since 1991, a law allows for access to the files of the Stasi, East Germany's former security service, by individuals and researchers. There have been two million requests from individuals for access to the files and three million requests for background checks since the archives became available. Researchers and the media have used the archives 15,000 times.

For other countries, a systematic declassification has also been found to be useful to keep the system running. The 1995 US Executive Order requires that all information 25 years and older that has permanent historical value be declassified by December 2006 unless it was specifically exempted and is subject to outside review. It changed the burden so that its costs the agency to not declassify information by making it justify why it should not be declassified rather than why it should be. It also set up a parallel system of oversight. Between 1995 and 2001, over 950 million pages were declassified, 100 million pages in 2001 alone.[29]

Conclusion and Recommendations

The Law on Protection of State Secrets is a relic of a less democratic era. It should be rescinded and replaced with more modern legislation that reflects the needs of the media and citizens of Kyrgyzstan to free access to information and expression.

The new law should be based on the principle that limits to the right of access to information should be specific, limited to only that which is necessary and set in the law. All withholding should be subject to strict harm and public interest tests based in the freedom of information act. There should be an adequate independent oversight regime.

The government should also take a forceful break from the past by ordering the declassification and release of documents from previous regimes, especially those that detailed abuses by the security services.

[28] See Hungary. Act XXIII of 1994 on the Screening of Holders of Some Important Positions, Holders of Positions of Public Trust and Opinion-Leading Public Figures, and on the Office of History. http://www.th.hu/html/en/torv.html; Lithuania, Law on Registering, Confession, Entry into Records and Protection of Persons who Have Admitted to Secret Collaboration with Special Services of the Former USSR. No. VIII-1436. November 23, 1999. As amended by June 13, 2000. No. VIII-1726. http://www3.lrs.lt/cgi-bin/getfmt?c1=w&c2=123807

[29] Information Security Oversight Office, 2001 Report to the President, September 2002.