Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Independent Oversight Authority for Intelligence Activities OA-IA

2024 Annual Report

of the Independent Oversight Authority for Intelligence Activities OA-IA

1 Summary

As in the previous year, the security situation in 2024 did not improve, but deteriorated. This created some new challenges for the intelligence services under the OA-IA's oversight. It also meant that the OA-IA had to be flexible and adapt its audit activities to the circumstances, in some cases redefining its priorities.

The need for the intelligence services to adapt to the evolving |security| situation was a major concern for the OA-IA. In addition to the Federal Intelligence Service (FIS), the Cyber and Electromagnetic Activities Service (CEA), which has carried out its intelligence activities since 2024 as part of Cyber Command, is also undergoing a transformation. Furthermore, the Armed Forces Preventive Protection Service (AFPPS), which is part of the Military Intelligence Service (MIS), is being expanded. Given its mandate from the FIS, this raises the question whether the OA-IA could and should also audit these activities as part of its legal mandate.

Oversight authorities must not only monitor but also understand technological developments in the field of intelligence. For this reason, the OA-IA has continued to invest in the training of its staff in 2024, whether through participation in conferences on current technical issues or through relevant further training. As international meetings with other oversight authorities have shown, technological developments and the need to adapt to changing circumstances as a result of these developments pose major challenges not only to the OA-IA, but also to other regulators.

In addition to the ongoing and completed audits of the FIS, one audit focused on the CEA and one on the MIS. With regard to the MIS, the OA-IA continued the interviews started in 2023 at management level on its oversight responsibilities vis-à-vis the AFPPS. The corresponding audit listed in the 2024 audit plan had not yet started at the time of writing.

2 Table of contents

3 Key figures as of 31 December 2024

Employees	1 January 2024	**9**
	31 December 2024	**9**
Ongoing audits as of 1 January 2024		**10**
Audits started in 2024		**9**
Audits concluded in 2024		**11**
Ongoing audits as of 31 December 2024		**9**
Planned audits		**10**
Unannounced audits		**1**
Recommendations		**14**

4 Personal remarks

What is the purpose of an audit?

Every activity has a goal. In some areas, achieving that goal produces a tangible result, such as a product or service. In other areas, it does not. The implementation of preventive measures in the field of national security is an example of an objective that does not necessarily produce a tangible (or measurable) result: if an attack is thwarted, it may not always be possible to determine whether this was the result of effective preventive measures or some other reason, such as the would-be perpetrator falling ill. As in all areas of life, there is a degree of luck involved.

Audits can also be considered a preventive measure. They do not necessarily lead to measurable findings, but rather to improvements in the system.

As the oversight authority for the intelligence services, we face the dual challenge of making our work tangible to the public and, above all, achieving measurable results in the form of improvements in the services we oversee. Did we achieve this in 2024? This report seeks to genuinely answer that question.

First, we had to reiterate the need for the FIS to strengthen its legal and management powers in order to provide a professional and harmonious working environment for its staff. The fact that we raised this issue in several areas shows that one audit was not enough. However, there are now signs of greater awareness and organisational developments in the right direction.

In the MIS, we found that risk management, for example in new crisis situations, works pragmatically in the daily work of employees, but is not yet established in administrative processes. The documentation is currently being revised. We are therefore monitoring this issue closely to ensure that management remains in touch with the day-to-day reality experienced by its staff.

Sometimes audits show that an area where we make a recommendation needs to be improved before other issues are addressed. We do not intervene indiscriminately, but carry out our audits based on an analysis of current or recurring risks. Services that are going to be audited sometimes make certain improvements in anticipation of an audit.

This report presents summaries of all our audits. This year, the summaries are accompanied by additional information to show the stages of our work, the time taken to reach our conclusions and the number of contacts we had with the audited services.

One final thought on the purpose of audits. Audits are used to promote positive developments, improve poor conditions, identify and correct problems and improve work processes. In other words, audits ensure that tasks are carried out in a professional way rather than based on luck.

I hope you enjoy our report.

Prisca Fischer, OA-IA Head

5 Oversight activities

5.1 Audit plan

The OA-IA performs risk-oriented audits in the following areas:

- Strategy and planning
- Organisation and tasking
- Cooperation
- Information gathering
- Resources
- Data processing and archiving

The audit plan is designed to ensure that each area is audited at least once a year.

5.2 Audits conducted in 2024

The OA-IA's annual report is continuously evolving and therefore contains some new features this year:

- The annual report contains a summary of each audit that was officially completed (i.e. confirmed by the head of the Federal Department of Civil Protection, Defence and Sport DDPS) by 31 December 2024. For ongoing audits, the report outlines their objective.

- Each audit summary contains a table with four time-related items of information: the date the audit started (mandate); the date the draft report was sent to the audited service for comments (consultation); the date of the final report; and the date the audit was officially completed. The table also indicates the duration of the audit (if completed) or its current status (if ongoing). Finally, the table indicates the number of interviews (oral or written) conducted up to 31 December 2024.

5.2.1 Strategy and planning

In the area of strategy and planning, the OA-IA examines issues relating to the short, medium or long-term strategic planning of the Swiss intelligence services and their objectives. The following audit was planned for 2024:

24-1 Artificial intelligence (AI) at the FIS

In this audit, the OA-IA is examining whether the FIS acquires, uses and controls this technology in accordance with the law and in terms of effectiveness and expediency. The OA-IA carried out preparatory work in 2024 and will conduct the actual audit in 2025.

5.2.2 Organisation and tasking

In the area of organisation and tasking, the OA-IA examines the adequacy of the structure and processes of the intelligence services and asks whether they enable the intelligence services to fulfill their mandate in a lawful, expedient and effective manner. In 2024, the OA-IA carried out the following audits in this area:

23-2 Legal services of the FIS

Mandate	Consultation	Final report	Official completion	Interviews conducted
10.08.2023	15.05.2024	05.08.2024	25.09.2024	40

Compliance with the law is particularly important in the field of intelligence. If the FIS or its employees do not act in accordance with the law, various fundamental rights – such as data protection, privacy or business confidentiality – may be violated. On the other hand, if the FIS does not make full use of the legal framework for conducting intelligence activities, Switzerland's security may be compromised and its reputation damaged, leading to a loss of public confidence in the institution. For this reason, the OA-IA decided to examine the effectiveness and expediency of the tasks, powers and responsibilities of those providing legal services at the FIS.

For this audit, the OA-IA interviewed members of staff from different sections and with different functions with five questions. It also inspected various documents. The OA-IA found that although the FIS provides mandatory training to its staff, the implementation of the training policy could be optimised in all organisational units following the transformation of the agency. Like other bodies of the Federal Administration, the FIS may draw on external expertise. However, in recent years, it has only awarded a few specific external mandates for legal services, suggesting that its own resources are sufficient.

Legal services are provided particularly by the organisational units responsible for quality assurance, compliance and legal services. The OA-IA found that there is a need for action in all three areas, or at least that certain areas require greater attention in light of the ongoing transformation.

The OA-IA made two recommendations concerning the activities of the Compliance Unit and their accountability, well as concerning the active involvement of the Legal Service in certain matters, and in the design of work processes. The current structure and competences of the Legal Service do not allow it to meet the requirements and expectations of the service. Addressing this will require more than simply updating the job description of the head of the Legal Service. The last formal compliance audits took place in 2021. At that time, only the Reporting Office was being actively managed by the Compliance Unit, but there is no record of this activity. With regard to the Quality Assurance Unit, has been a high turnover of legally trained staff, who need to be replaced as soon as possible in order to address the backlog of work in updating documentation.

23-4 IT Service Continuity Management (ITSCM) and Disaster Recovery at the FIS

Mandate	Consultation	Final report	Official completion	Interviews conducted
13.02.2023	11.01.2024	06.02.2024	06.04.2024	4

In this audit, the OA-IA examined whether the FIS has effective and appropriate procedures in place to deal with emergencies in IT operations, so that the critical business processes of the FIS can be guaranteed and its data recovered.

Major unforeseen incidents such as fires, floods and criminal activity pose a threat to every organisation and can cause damage – particularly to IT infrastructure – that is far worse than a simple loss of service. Organisations therefore need to ensure that they have business continuity management (BCM) in place, which analyses the risks posed by an incident with the aim of minimising its impact on critical services and business processes.

Given the heavy reliance of business operations on information technology, the existence of a resilient IT infrastructure is essential to the survival of an organisation. ITSCM, together with BCM, ensures that even in the event of major incidents, the IT services that the organisation has identified as critical can be delivered. It does this by assessing and implementing measures to be adopted in the event of an incident (strengthening resilience and response). ITSCM must ensure that information and communications technology (ICT) services and infrastructure are available after a failure or can be restored within an agreed period. IT Disaster Recovery, on the other hand, aims to restore ICT services and infrastructure after a failure.

Effective ITSCM must take into account current and specific risks. With increasing digitalisation and data processing at the core of FIS's activities the status of data processing as the core activity of the FIS – and against the backdrop of potential energy shortages, increasing cyberattacks and a war in Europe – the FIS is more dependent than ever on the continuous and reliable operation of IT infrastructures. Furthermore, data loss threatens the FIS's ability to fulfill its mandate.

BCM has already been the subject of a report by the DDPS Internal Audit (Report I 2022-01 of 15 August 2022). One of the recommendations in the report called on the DDPS administrative units to update their BCM documentation. The FIS is working on the implementation of this recommendation. In addition, the management of the FIS has decided to wait until its transformation is complete before approving and implementing a new BCM plan. The OA-IA has therefore taken a cautious approach to BCM issues.

The OA-IA found that certain ITSCM documentation was missing due to insufficient ITC governance within the FIS. Measures have been taken in this area, but only at a technical level. The FIS ICT unit has taken numerous measures to ensure business continuity in the event of a major incident. The planned measures are effective and proportionate to the situation. In particular, they ensure the redundancy of the ICT infrastructure and data security strategy, and minimise risks. However, there is no testing strategy, so it is not certain that the ICT delivery service would actually maintain its high level of stability in the event of a major incident. Furthermore, the ITSCM plan cannot be updated without extensive and regular testing. Recommendations were made in relation to ITSCM documentation and the organisation of testing.

24-2 Intelligence activities by the Armed Forces Preventive Protection Service (AFPPS)

The aim of this audit is to examine the cooperation interfaces between the FIS and the AFPPS in order to identify intelligence activities. The OA-IA will therefore examine the legality, effectiveness and expediency of the cooperation between these two services.

In 2024, several interviews were conducted regarding the OA-IA's responsibility for the oversight of the AFPPS (see 6.4). The actual audit will take place in 2025.

24-3 Organisation of partner service contacts at the CEA

Mandate	Consultation	Final report	Official completion	Interviews conducted
15.05.2024	12.11.2024	27.11.2024	02.12.2024	9

No intelligence service can identify and avert all threats on its own. Close and confidential cooperation with partner services is therefore essential. This also applies to the intelligence services in Switzerland and thus to the CEA. The fact that the CEA is a relatively small service, is not integrated into multilateral bodies (e.g. SIGINT Seniors Europe) and does not have access to all signal flows in the same way as other countries due to Switzerland's geographical location, makes the CEA's tasks particularly difficult. This makes bilateral contacts at the operational level with selected partner services all the more important.

These contacts are based on a give-and-take approach. When the CEA receives information from a partner service, it provides information of interest to that partner service in return.

Although this exchange is essential for the CEA, it involves risks and raises some questions. For example, the nature of the information exchanged could lead to unlawful actions on the part of the service. In addition, the process and the way in which contacts with partner services are managed also pose risks in terms of effectiveness and expediency.

For this reason, the OA-IA decided to review the contacts between the CEA and its partner services in 2024.

With regard to the legal issues, the OA-IA concluded that the CEA complies with the legal requirements and that it only maintains intelligence-related contacts with its partner services on behalf of the FIS. The vast majority of contacts with partner services are of a technical nature. When sensitive data are exchanged, the FIS Legal Service verifies the legal basis for the respective data exchange in advance.

With regard to the effectiveness and expediency of the CEA's contacts with partner services, the OA-IA concluded that the existing ones are organised and carried out effectively under the given circumstances. The approach to developing future partner service contacts in the areas of cyber and electromagnetic activities also appears to be effective and efficient. From a purely technical point of view, participation in international bodies in the field of SIGINT would promise more efficient partner service contacts. However, this cannot be decided at the level of the CEA or the FIS, but requires a fundamental political decision.

Based on the overall findings that the CEA strictly adheres to the legal framework and makes the best of its contacts with partner services, the OA-IA did not make any recommendations.

24-11 Security aspects under Article 6 paragraph 7 of the Federal Act of 25 September 2015 on the Intelligence Service (Intelligence Service Act, IntelSA, SR 121)

Mandate	Consultation	Final report	Official completion	Interviews conducted
16.10.2024				2

The FIS has a duty to protect its staff, facilities, sources and the data it processes. The OA-IA decided to audit how the FIS fulfils this obligation in certain areas.

This audit was not announced and will be completed in 2025.

5.2.3 Cooperation

The OA-IA examines cooperation between the intelligence services and national and international authorities. To this end, it audits individual cantonal intelligence services (CISs) every year. With the audit reports on Nidwalden (23-6 CIS NW) and Obwalden (23-7 CIS OW) and the publication of the summaries on the website, the OA-IA has now completed its audit of all 26 cantons and can draw a conclusion.

In the area of cooperation, the following audits were carried out in 2024:

23-6 Cantonal Intelligence Service Nidwalden (CIS NW)

Mandate	Consultation	Final report	Official completion	Interviews conducted
16.11.2023	15.02.2024	20.03.2024	10.04.2024	2

The OA-IA examined whether the cooperation between the FIS and the CIS NW is lawful, effective and expedient. It concluded that the FIS and the CIS NW cooperate well and that the CIS NW generally responds to FIS requests in a timely and substantive manner. However, the OA-IA had the impression that the CIS NW was not sufficiently aware of the need to separate the infrastructure of the cantonal police and the CIS. This creates a risk of information leaks. The OA-IA therefore made a recommendation to this effect.

The OA-IA also examined whether stored data, and personal data, stored met the legal requirements in terms of relevance to the task, compliance with the data processing restrictions, and the accuracy and relevance of the information. The OA-IA found that outstanding data storage issues or technical issues relevant to data protection are not handled with the necessary diligence, and that it is not always possible to understand or trace the relevance of a task due to staff turnover. This creates a risk of unlawful data processing or leakage of information. The OA-IA has made a recommendation to this effect.

23-7 Cantonal Intelligence Service Obwalden (CIS OW)

Mandate	Consultation	Final report	Official completion	Interviews conducted
16.11.2023	15.02.2024	29.03.2024	16.04.2024	2

The OA-IA examined whether the cooperation between the FIS and the CIS OW is legal, appropriate and effective. The OA-IA concluded that the FIS and the CIS OW cooperate well on current issues and that communication also operates at low-threshold. The CIS OW fulfils the FIS's mandates on time, as expected in terms of contents, while preserving resources. The OA-IA gained the impression that the CIS OW has good intelligence capabilities and the necessary qualities, as well as the conditions and motivation to fulfil its tasks.

The OA-IA also checked whether stored data, including personal data complied with the legal requirements in terms of relevance to the task, restrictions on data processing and the accuracy and relevance of the information. The OA-IA did not find any irregularities in this respect.

CIS audits in recent years

Between 2019 and 2024, the OA-IA carried out an audit of all 26 CISs. The basic audit strategy was the same for all CISs, but with additional, specific questions for each canton.

For 11 CISs there were no concerns. For the remaining 15, the OA-IA issued a recommendation particularly to improve CISs' data processing, resource management and the use of technical tools. All of the recommendations have been implemented, except for one, for which the deadline has not yet expired. Thanks to the measures taken by the FIS, some of the concerns raised by the OA-IA over the years have not been repeated. The OA-IA also found that a recommendation made to one canton sometimes also had an impact on other cantons.

Through these audits, the OA-IA has acquired detailed knowledge of the CISs, their activities and their individual characteristics. Some cantonal oversight authorities regularly send their oversight reports to the OA-IA, which provides the OA-IA with additional information.

The OA-IA has decided that, in future, CIS audits will no longer be based on standardised audit questions, but on risk-based considerations relating to specific topics in the individual cantons (see 7.1, OA-IA visits to the cantons).

23-10 Cooperation between the FIS and private actors

Mandate	Consultation	Final report	Official completion	Interviews conducted
05.09.2023	02.07.2024	15.08.2024	16.12.2024	7

The FIS cooperates with private actors. These can be private individuals, organisations or companies. This cooperation in the administrative field is based primarily on the usual contractual relationships. In the operational field, it takes place with private individuals (known as 'supporters'), who assist the FIS in fulfilling the tasks defined in Article 6 IntelSA.

Initially, the OA-IA investigated an issue that had been raised during an inspection by the Swiss Federal Audit Office (SFAO) concerning administrative cooperation between the FIS and private actors. To this end, the OA-IA carried out spot checks on several ongoing service contracts between the FIS and various companies. It also carried out sampling on payments in the FIS's accounts, including covert payments to undercover sources, which are present in the FIS accounts. In a second step, the OA-IA expanded its audit to payments made to individuals (supporters) for operational cooperation.

In particular, it analysed the legality of the mandates given by the FIS to private individuals according to the criteria defined in the IntelSA and IntelSO (Intelligence Service Ordinance). It also analysed the expediency and effectiveness of cooperation with supporters by examining the FIS's portfolio management and the lifecycle management of these supporters.

The OA-IA also analysed risk management and tested various assumptions. This included looking at whether measures that generally require authorisation had been circumvented by giving mandates

to private individuals, unlawful behaviour by private individuals, payments made without consideration, and cooperation with private individuals whose reputation could damage the FIS.

The OA-IA found that the FIS's supervision of private actors and its follow-up documentation were adequate and that there had been improvements in this area. However, it found that there was room for improvement in the handling of security breaches by private actors. It concluded that the practice of delegating certain operational tasks to private actors should be clarified. The OA-IA drew the attention of the FIS to these points, without making any recommendations.

24-4 Cooperation between the FIS and the State Secretariat for Migration (SEM)

Mandate	Consultation	Final report	Official completion	Interviews conducted
17.05.2024	18.12.2024			15

The OA-IA reviewed the cooperation between the FIS and SEM and examined whether their exchange of data is legal, effective and expedient.

5.2.4 Information gathering

Information gathering is a core task of the intelligence services. Various means can be used for this purpose. The OA-IA pays special attention to those that most deeply intrude into the privacy of the persons concerned. Every year, the OA-IA examines operations (OP) and intelligence gathering through human sources (HUMINT) due to the risks associated with these activities. In 2024, the OA-IA carried the following audits in this area:

23-11 FIS operations, operational clarifications and information-gathering activities requiring authorisation

Mandate	Consultation	Final report	Official completion	Interviews conducted
04.05.2023	18.01.2024	13.02.2024	05.03.2024	4

Intelligence service operations (OPs) and operational inquiries (OPIs) are among the core tasks of the FIS. They are more complex than day-to-day operations and require operational management. OPs may involve information-gathering activities that require authorisation. The OA-IA regularly reviews OPs and OPIs, as their complexity often poses risks with regard to their effectiveness and expediency. It also regularly examines information-gathering activities that require authorisation, as these always involve a legal risk due to their invasion of privacy.

The OA-IA found no significant changes in the volume of OPs and OPIs compared to the previous year, nor in the topics covered. This year again, the FIS sought to terminate long-running OPs and OPIs. The OA-IA considers that this approach is appropriate and should be continued in the future.

On the basis of its controls, the OA-IA found nothing to indicate that the five OPs and eleven OPIs had not been carried out in a legal, effective and expedient manner.

The OA-IA also examined whether the relevant decisions of the Federal Administrative Court (FAC) had been implemented in the case of eight authorised information-gathering activities, three urgent measures and one rejected measure. On the basis of the audits, the OA-IA had no reason to believe that the measures had not been carried out in compliance with the authorisation process. Nor was there any evidence to suggest that the FIS had unlawfully carried out measures despite the refusal of authorisation.

Based on this overall positive impression, the OA-IA decided not to make any recommendations.

23-12 Human intelligence (HUMINT) in the FIS

Mandate	Consultation	Final report	Official completion	Interviews conducted
11.08.2023	07.03.2024	01.05.2024	26.06.2024	30

Human intelligence is an area where secrecy is a cornerstone of the activity. It requires particularly strict security and protection measures with regard to employees (including the use of alias

identities or cover stories to conceal their association with the FIS) and their place of work, the financial flows necessary to conceal the origin of payments, the obligations to protect sources, etc. The risks in these areas are numerous and constantly increasing, which justifies an annual audit by the OA-IA.

In view of the transformation and the strategic reorientation of the FIS, the main objective of the OA-IA was to determine the status of the HUMINT division prior to the transformation of the agency. In the context of audit 23-12, the OA-IA was therefore particularly interested in the development of the source portfolio, be it in strategic terms, in terms of HUMINT personnel, development and learning capacities, or in terms of ongoing projects. The audit also provided an opportunity to take a snapshot of the functioning and difficulties of the HUMINT division prior to the agency's transformation. To this end, oral or written interviews were conducted with all HUMINT staff. The OA-IA found that although the staff were generally satisfied with their work and highly motivated, the transformation of the FIS was exacerbating a number of pre-existing difficulties already identified by the OA-IA.

The development and digitalisation of society in general are further factors that increase pressure on areas that require secrecy. Ongoing projects, such as a new training programme for source handlers and a new documentation management system, should provide effective solutions. Overall, the HUMINT division has the necessary skills, ideas, human resources and motivation to resolve current problems. The OA-IA has made two recommendations concerning human resources management and the evaluation of information provided by sources.

Finally, the audit found that the areas controlled were managed in accordance with the law and adequately documented.

23-13 Use of undercover cyberagents in the FIS

Mandate	Consultation	Final report	Official completion	Interviews conducted
14.05.2024	21.11.2024			10

The global threat situation has changed. In the field of terrorism and violent extremism, communication has shifted from publicly accessible platforms such as Facebook to encrypted communication services and closed communities.

As a result of this evolving situation, the FIS's use of virtual cover identities to monitor the internet for terrorist or violent extremist activity is becoming less effective, as this tool is primarily used to cover the public domain and does not allow access to [encrypted] communication services and closed communities. To gain access to these services and groups, the FIS needs undercover cyberagents. By establishing contact with potential targets, undercover cyberagents build up enough trust to gain access to these closed forums.

For this reason, the OA-IA examined whether the legal framework for the use of undercover cyberagents is clear and understood by the staff involved. It also examined whether the training of cyberagents in the FIS was adequate and their deployment appropriate.

The OA-IA also examined whether the FIS has the technical and organisational framework to deploy cyberagents effectively and to correctly assess the chances of obtaining intelligence successfully from the outset.

24-5 FIS operations, operational clarifications and intelligence-gathering measures requiring authorisation

Mandate	Consultation	Final report	Official completion	Interviews conducted
25.07.2024				10

In this ongoing audit, the OA-IA is examining whether the new organisational structure of the FIS will ensure the legality, effectiveness and expediency of operations. To this end, it is reviewing a selected

number of OPs and OPIs. It is also examining a number of authorised information-gathering activities to ensure that they are being implemented in compliance with the relevant rulings of the FAC.

24-6 Human intelligence in the FIS

Mandate	Consultation	Final report	Official completion	Interviews conducted
29.10.2024				1

In this ongoing audit, the OA-IA is examining two main aspects. The first is a follow-up to audit 23-12 and looks at the question of how the FIS has responded to some of the critical issues raised by the OA-IA in its report. The second aspect looks at whether the management of sources (human sources and 'supporters') is being documented in a lawful and expedient manner.

5.2.5 Resources

In the area of resources, the OA-IA examines whether the intelligence services are using their resources wisely and whether intelligence activities are being carried out effectively. In 2024, the OA-IA carried out the following resource audits:

24-7 Information and communication technology inventory (ICT) in the FIS

Mandate	Consultation	Final report	Official completion	Interviews conducted
22.10.2024				

In ICT, it is important for an organisation to have an overview of the hardware it uses for a number of reasons. This overview helps to manage hardware components throughout their lifecycle, thereby ensuring optimal use of resources. In addition, a systematic inventory prevents hardware from being procured and used by unauthorised individuals within the organisation. For the FIS, this last point in particular poses both a reputational risk and a risk of unlawful data processing due to a lack of control mechanisms.

For this reason, the OA-IA decided to examine whether the FIS has an inventory of its hardware and, if so, whether this inventory is being managed effectively and expediently. The aim of this is to determine whether hardware components have been procured or used unlawfully, and to prevent this from happening in the future.

The audit is not focusing on the entire ICT inventory of the FIS, but only on the IT hardware used in connection with the collection and processing of data.

24-8 Incident and risk management in the MIS

Mandate	Consultation	Final report	Official completion	Interviews conducted
30.01.2024	11.06.2024	10.07.2024	23.07.2024	6

Due to their covert nature, intelligence activities often involve risks. These risks relate, in particular, to the organisation of the work, which may result in an involuntary leak of information and therefore lead to a security threat or reputational damage. However, the legal or political aspects of intelligence activities can also pose risks for which the organisation carrying out the intelligence activity is responsible. This is where risk management plays a critical role. Risk management is the process of identifying an organisation's risks, taking appropriate measures to reduce them, and limiting any potential damage. How an organisation deals with incidents that result from identified risks or that affect the general security of an organisation is an important question and is known as incident management.

If risk management is absent or inadequate, an intelligence service may be limited in its ability to carry out its intelligence tasks, thereby losing its effectiveness and relevance. At worst, this could result in an intelligence service such as the MIS no longer being able provide services to the Swiss Armed Forces.

For this reason, the OA-IA decided to audit the risk and incident management of the MIS.

In the area of risk management, the OA-IA found that the MIS has a complete overview of the key risks. However, optimal risk management requires a structured approach to managing these risks. This includes, among other things, the updating of documents, the regular exchange of information on the development to risks, and a discussion of action to be taken. In the opinion of the OA-IA, this does not currently happen sufficiently in the MIS. However, a new risk strategy will address this shortcoming in 2024.

With respect to incident management, the OA-IA found that the MIS consistently records security-related incidents that could cause or increase risks arising from intelligence activities. The OA-IA also found that the MIS deals with these incidents and incorporates them into its risk management. However, to date the MIS has had to deal with relatively few incidents. This could lead to a false sense of security. The OA-IA has therefore concluded that any new risk strategy should include exercises on responding to serious security incidents.

Due to its sound risk management, the relatively low number of security-related incidents and the fact that MIS personnel have a heightened risk awareness due to their military background, the OA-IA did not formulate any recommendations.

5.2.6 Data processing and archiving

In the area of data processing and archiving, the OA-IA verifies the legality of information processing. This is because the information processed by intelligence services is highly sensitive and the legal requirements are both extensive and complex. In 2024, the OA-IA conducted the following audits in this area:

22-15 Open-source intelligence (OSINT) in the FIS

Mandate	Consultation	Final report	Official completion	Interviews conducted
29.12.2022	07.12.2023	14.02.2024	08.03.2024	11

Open-source intelligence is a rapidly developing area of intelligence. The collection of seemingly infinite amounts of open-source information provides intelligence services with almost endless opportunities to generate intelligence. The analysis of this information, with the aim of extracting useful information is referred to as open-source intelligence (OSINT). In addition, the collection of open-source information does not require authorisation (Art. 13 IntelSA), which allows the FIS to search for intelligence-relevant data in a large volume of information. The growing importance of OSINT is raising legal and ethical questions within the international intelligence community, such as where to draw the line between OSINT and HUMINT, particularly with regard to the use of online identity aliases to investigate persons of interest or to obtain data sets offered illegally on the internet (leaks). The OA-IA therefore decided to examine the use of OSINT by the FIS.

According to Article 13 IntelSA, public sources of information include publicly accessible media, publicly accessible registers of federal and cantonal authorities, personal data made publicly accessible by private individuals and statements made in public. The boundary between OSINT and information-gathering measures requiring authorisation is not always clear, and this issue is also a subject of discussion among the FIS's partner services and foreign oversight authorities. If there is no common understanding of these boundaries, there is a risk of unlawful intelligence gathering. The interviews conducted with FIS OSINT staff revealed that they are aware that they are operating in a complex legal situation with regard to OSINT. However, there are no criteria or structured guidelines as to what constitutes OSINT and where the legal limits of OSINT lie. As a result, the FIS does not clearly and consistently regulate the use of different OSINT activities. The OA-IA therefore made a recommendation to define the legal framework for the collection of OSINT-related information and uniform rules for the use of OSINT.

The OA-IA reviewed selected cases of OSINT-related information gathering and found no evidence of unlawful activity. The FIS is required to provide evidence of its own activities through a systematic records management. All business-related documents must be registered and filed in the FIS GEVER business management system. The OA-IA found that some cases of OSINT-related information collection had been insufficiently documented and did not comply with the applicable Federal

Administration regulations, making it impossible for the OA-IA to assess its legality. The OA-IA issued a recommendation in this instance.

OSINT tools are used to efficiently and effectively generate intelligence-relevant information from the huge amount of data available through publicly accessible online sources. The FIS uses a mix of standard, commercially available products and in-house developments that enable the use of online identity aliases for continuous monitoring and targeted searches. Online identity aliases present particular features due to their use by intelligence services and could therefore be identified as potential targets by other agencies and become the focus of partner services. To counter this risk, the OA-IA proposed that the FIS and the CISs should inform each other about the online identity aliases they use.

The FIS uses a dedicated IT infrastructure for the collection of anonymised OSINT-related information. This infrastructure has security vulnerabilities and should be upgraded or replaced in the near future. The OA-IA has made a recommendation to this effect.

It can be difficult to verify the results of OSINT research, particularly in the case of information found on the Darknet. The FIS considers it an integral part of intelligence work to treat information with an appropriate degree of suspicion. If information cannot be verified or its veracity cannot be quantified, this is noted in OSINT reports. Source verification, which plays an important role in detecting and exposing fake news, for example, is a particularly well-known problem in the use of complex commercial OSINT products and is also a recurring theme within the intelligence community.

In addition to the FIS, the CISs also conduct OSINT research. The OA-IA therefore examined possible duplication and inefficiency. It concluded that the agencies were aware of the risks and had taken steps to address them, for example by ensuring regular discussion of OSINT in a recently established forum.

The FIS uses the OSINT information system (OSINT Portal) to make data from public sources available internally. During its audit, the OA-IA found no evidence that the OSINT Portal compromised the expediency or effectiveness of data management. OSINT data has a shorter retention period than data generated by other sensors. This eliminates the risk of OSINT data being mislabelled, resulting in an unlawful extension of the data retention period.

22-18 Information gathering by the FIS CYBER division

Mandate	Consultation	Final report	Official completion	Interviews conducted
07.06.2022	18.11.2024			17

The time-consuming audit concerning unlawful data collection by the FIS Cyber division was completed in 2024. As report writing also proved to be quite difficult, the consultation process was still ongoing when this annual report went to press. The OA-IA will therefore publish a summary of the facts and findings of the audit on its website in 2025 and report on it in detail in the next annual report.

23-16 Information systems, data storage systems and data files outside the scope of Art. 47 IntelSA

Mandate	Consultation	Final report	Official completion	Interviews conducted
17.07.2023	18.03.2024	06.05.2024	05.06.2024	7

Since its establishment, the OA-IA has carried out annual audits of the FIS's information systems. Data processing is fundamental to the activities of the FIS: if data are not processed correctly or are not available to employees for analysing the security situation, the FIS may not be able to perform its tasks. The information systems used by the FIS for its intelligence activities were regulated for the first time under a single legal provision – Article 47 – with the entry into force of the Federal Act of 25 September 2015 on the Intelligence Service (IntelSA).

The OA-IA's audit revealed that the FIS operates other information systems in addition to those listed in Article 47 IntelSA. As the question arose during the drafting of the legislation as to whether all

systems were listed in Article 47, the OA-IA decided to clarify the matter. It found that the list is exhaustive as far as data in systems used for intelligence activities in the strict sense are concerned: these data must be saved in one of the information systems listed in Article 47.

The OA-IA then examined which other systems are used, for what purposes and whether the legal provisions are adequate. It concluded that the legal provisions governing the operation of the other systems were adequate.

With so many FIS systems in use, it is important that each one is fully and properly managed. It is particularly important to have an accurate and up-to-date overview of all systems in use to ensure that data processing is lawful at all times. The audit concluded that the overview of systems operated outside the scope of Article 47 IntelSA needs to be updated and better managed. This overview needs to be shared with the Board of Directors, Quality Control and the technical teams so that the data can be properly stored and checks can be carried out. The OA-IA therefore formulated an appropriate recommendation.

24-9 Spot check of the Information and Analysis System All-Source Integral Control Centre (IASA-ICC)

Mandate	Consultation	Final report	Official completion	Interviews conducted
09.12.2024				

The OA-IA is currently examining the legality, effectiveness and expediency of the data contained in the IASA-ICC database through random checks and interviews. The audit is ongoing.

24-10 FIS searches in third-party information systems

Mandate	Consultation	Final report	Official completion	Interviews conducted
10.06.2024				5

The OA-IA is currently examining whether the FIS's access to third-party information systems and searches made in these databases are lawful and expedient. The audit is ongoing.

5.3 Acceptance

The OA-IA's auditors were received by the audited units in a constructive and professional manner. They were given direct access to the documents and information systems needed to carry out their audit tasks. The auditors also had no difficulty in contacting interviewees whenever they needed to do so and additional questions were answered as quickly as possible.

5.4 Implementation of the recommendations

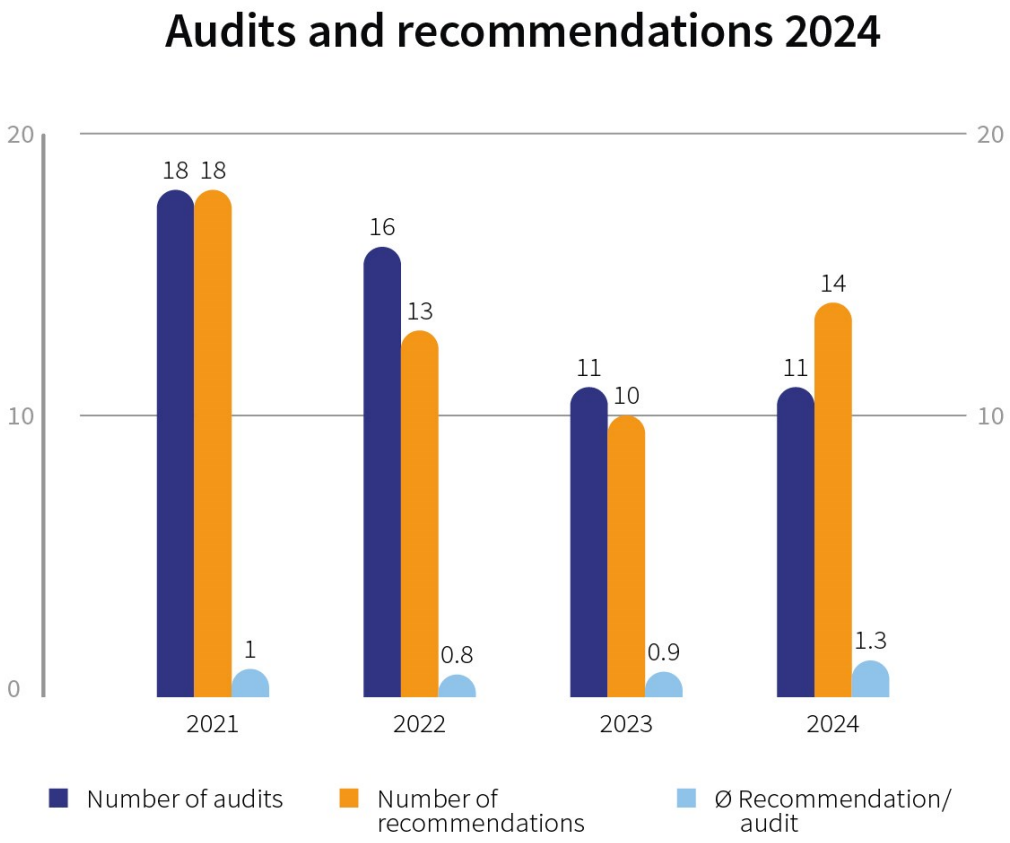
Based on its audit activities, the OA-IA can make recommendations and submit them to the head of the DDPS. The DDPS then ensures that these recommendations are implemented. If the DDPS rejects a recommendation, it must submit it to the Federal Council for a decision. To date, no recommendations have been rejected.

The OA-IA has no legal authority to monitor the implementation of recommendations. However, effective and credible oversight is only possible if the implementation of recommendations is correctly applied and monitored. The OA-IA carries out this part of its oversight function in dialogue with the audited units and the DDPS.

The following table shows the relationship between the number of audits carried out over the last four years and resulting recommendations.

After an initial three-year period (2018-20), in which an average of three recommendations were issued per audit, only around one recommendation was made per audit from 2021 onwards. This is a result of the OA-IA's consistent approach of issuing fewer, but more targeted and effective recommendations. The number of recommendations does not indicate whether conditions are improving or deteriorating.

	2018-2020	2021	2022	2023	2024
Number of audits	49	18	16	11	11
Number of recommendations	150	18	13	10	14
Ø Recommendation/Audit	3.1	1.0	0.8	0.9	1.3



6 News from the OA-IA office

In this chapter, the OA-IA reports on internal matters.

6.1 Personnel

In 2024, the OA-IA had nine staff members. One person left and was replaced by a new member of staff.

6.2 Training and professional development

Over the course of 2024, the OA-IA's staff participated in numerous training and professional development courses offered by the federal government or private institutions, particularly in the areas of risk management, auditing, cybersecurity and personal development. In addition, two staff members successfully completed Certificate of Advanced Studies (CAS) courses in communication and in artificial intelligence management.

6.3 Access to official documents and information

The OA-IA works on behalf of the public as part of the decentralized Federal Administration. The public has the right to know what the authorities are doing and how they are fulfilling their mandate. This gives rise to the public's right of access to information and to the authorities' obligation to provide it.

During the year under review, the OA-IA received 11 requests for access to information held by the OA-IA itself. In six cases, access was refused, in two cases it was partially granted, and in two cases it was fully granted. In a further case, the OA-IA was asked for assistance in dealing with a request under the Federal Act of 17 December 2004 on Freedom of Information in the Administration (Freedom of Information Act, FoIA, SR 152.3), which had been addressed to another body of the Federal Administration.

6.4 OA-IA responsibility for the oversight of the AFPPS

During the consultation procedure on the 2024 audit plan, the question arose as to whether the OA-IA was responsible for the audit '24-2 Intelligence activities of the Armed Forces Preventive Protection Service (AFPPS)'.

In 2024, the head of the DDPS informed the OA-IA that she had submitted this question to the Federal Office of Justice (FOJ), which confirmed that the OA-IA is authorised to exercise oversight over the AFPPS in three situations:

- when the AFPPS carries out a mandate from the MIS
- when the AFPPS carries out a mandate from the FIS
- when the AFPPS carries out activities that also serve to fulfill tasks pursuant to Articles 99 and 100 of the Federal Act of 3 February 1995 on the Armed Forces and Military Administration (Armed Forces Act, ArmA, SR 510.10), or when it is not possible in practice to determine whether an activity serves a task pursuant to Articles 99 and 100 ArmA.

The head of the DDPS also informed the OA-IA that the question of responsibility could be addressed when the Armed Forces Act is revised in 2029.

The OA-IA took note of the FOJ's opinion, which was largely consistent with its own legal assessment. It concluded that the FOJ had not questioned Audit 24-2, the main objective of which was to verify the cooperation between the FIS and the AFPPS. The OA-IA stated that it would also take the FOJ's legal opinion into account when planning future audits.

6.5 Revision of the Intelligence Service Act

The revision of the IntelSA, which started in 2020, is on track. It has been divided into two parts. The first part mainly concerns data processing by the FIS and oversight activities. The consultation process took place in the summer of 2022, and the Federal Council is expected to adopt the dispatch on the basic part for submission to Parliament by the end of 2025. The OA-IA is significantly affected by this part of the revision, as it provides for the transfer of tasks from the Independent Control Authority for Radio and Cable Communications Intelligence (ICA) to the OA-IA. As part of the internal consultation process within the DDPS, the OA-IA requested that the relevant standards be amended. These amendments are intended to improve the readability of the law, to clearly define oversight activities and to incorporate new data protection requirements.

The second phase involves adapting the provisions on the processing of cyberdata. A supplementary consultation is to take place by July 2025.

7 Coordination

The OA-IA coordinates its activities with those of parliamentary oversight bodies as well as with those of other federal and cantonal oversight bodies, in accordance with Article 78 paragraph 2 IntelSA.

7.1 National contacts

Control Delegation (CDel)

The CDel invited the OA-IA to one hearing. The topics discussed were the OA-IA’s practice on issuing and monitoring recommendations, the revision of the Intelligence Service Act and the 2025 audit plan.

Federal Administrative Court (FAC)

Representatives of the FAC and the OA-IA met twice during the year. At these meetings, the FAC's practice with regard to intelligence activities requiring authorisation and requests for cable communications interception were discussed, and the OA-IA's current audits and 2024 audit plan were presented. In addition, the OA-IA's inclusion in the approval procedure was clarified and individual points concerning the revision of the IntelSA were discussed. The FAC's practice of dealing with technical problems was shown to be effective, as problems hardly ever arise anymore. With regard to the revision of the IntelSA, the head of the OA-IA went back on its recent proposal that it cross-checks the FAC's annual report. The FAC agreed.

Swiss Federal Audit Office (SFAO)

The OA-IA coordinates its oversight activities with other control authorities, in particular with the SFAO.

In this context, and following the SFAO's assessment of the service contracts between the FIS and private providers, the OA-IA and the SFAO established a clear line of coordination. With regard to Audit 23-10, the OA-IA examined the cooperation between the FIS and private actors, focusing mainly on covert operations, which are not covered by the usual service contracts. The audit 23-10 provided an opportunity to examine unlegended service contracts, but also the implementation of the SFAO's recommendation. No significant problems were found in the management of service contracts. The OA-IA subsequently communicated the relevant points of its report to the SFAO for information and follow-up.

In view of the major transformation that the FIS is currently undergoing, the OA-IA has intensified its dialogue with the SFAO. This is reflected in the exchange of audit findings and the optimisation of resources by avoiding duplicate audits.

This increased coordination reflects the desire of both oversight authorities to ensure comprehensive and efficient oversight of the FIS. It helps to verify compliance with recommendations and to closely monitor the transformation of the FIS.

Independent Control Authority for Radio and Cable Communications Intelligence (ICA)

During the year under review, a meeting was held between the president of the ICA and the head of the OA-IA. Discussions included an exchange with the FAC and a possible meeting between the ICA and a foreign regulator on cable communications surveillance.

A representative of the OA-IA also attended all five meetings of the ICA in connection with the planned transfer of oversight activities from the ICA to the OA-IA as part of the revision of the IntelSA. The purpose of attending these meetings was to gather information on the ICA’s audit methodologies and to ensure the transfer of expertise.

Federal Data Protection and Information Commissioner (FDPIC)

At a coordination meeting in 2024, the OA-IA informed the FDPIC of the main findings of the audits it had completed, as well as the ongoing and planned audits as far as they related to data processing. The meeting also dealt with the implementation of the right of access to information under the IntelSA.

OA-IA visits in the cantons

After the entry into force of the IntelSA, the OA-IA conducted a survey among the cantonal oversight authorities on the CISs and organised a first conference with them to discuss the results. The cantons participated in large numbers (see OA-IA 2018 annual report). In August 2021, the OA-IA organised a second conference for training, networking and sharing experiences. The number of participants was smaller so specific topics could be discussed in greater depth (see OA-IA 2021 annual report).

The OA-IA began its visits in the cantons in the summer of 2024. This cycle of visits will continue until early summer 2025. The dialogue partners include the heads of the various CISs and possibly some CIS staff, as well as the respective cantonal oversight authorities, which takes many forms in the Swiss federal system.

Discussions on the following topics are planned:

- OA-IA feedback on its first round of CIS audits;
- Current intelligence-relevant topics of interest to the CISs and cantonal oversight authorities;
- Coordinating any possible duplication of efforts by the various oversight authorities (FIS, OA-IA, cantonal oversight authorities and others), possible need for oversight and any open questions from the cantonal oversight authorities;
- Cooperation between the CISs and the cantonal oversight authorities.

So far, the cantons have welcomed the visits, and the discussions have been valuable. At the end of the visits, the OA-IA will produce a report and discuss any issues of concern in more detail with the FIS.

Other meetings

- Chief of the Armed Forces
- Head of the DDPS General Secretariat
- Deputy Head of the DDPS General Secretariat
- Director of the FIS
- Chief of Joint Operations Command
- Head of the MIS
- Head of the CEA
- Head of DDPS Internal Revision
- Attorney General of Switzerland
- President of the Supervisory Authority for the Office of the Attorney General of Switzerland (SA-OAG)
- Director of the SFAO
- Head of SFAO Mandates
- DDPS Intelligence Advisor
- ICA members

Enquiries from the public

The OA-IA received 16 enquiries from the public in 2024.

7.2 International contacts

The OA-IA can share audit methods, processes and experience with foreign oversight authorities working in the same field. This brings continuous benefits to audit activities. In 2024, the following international meetings took place:

Intelligence Oversight Working Group (IOWG)

IOWG Technical Meeting and Staff Meeting from 10 to 12 April 2024 in Brussels

The regular staff meeting was preceded for the first time by a technical meeting organised by the Belgian hosts. This new exchange platform was mainly attended by specialists with extensive technical knowledge from the oversight authorities. The focus of this first meeting was on artificial intelligence (AI) and included the following aspects:

- What do oversight authorities understand by AI?
- Do the applicable laws already take into account the use of AI or machine learning?
- Do intelligence services subjected to oversight already use this technology?
- Does the use of this technology fall within the supervisory remit of oversight authorities?
- Do oversight authorities themselves actively use this technology for their own needs?
- How can the oversight authorities ensure that knowledge about new technologies is preserved and developed?

The exchange between the specialists proved to be very enriching, and the technical meetings will continue on a regular basis.

The technical meeting was followed by a staff meeting with representatives from the oversight authorities of Belgium, Denmark, the Netherlands, Norway, the United Kingdom, Sweden and Switzerland. The Canadian authority NSIRA, which has observer status, was also represented.

At the beginning of the meeting, the participants presented various intelligence-related developments that had taken place in their country since the last meeting in 2023. Lively discussions took place on the following topics:

- The oversight of intelligence service investigations of politicians and elected officials, using the example of a case that is currently in the public eye in Belgium.
- European Data Protection Convention 108+ regulating the protection and cross-border exchange of personal data. Each participating country provided information on its ratification status. There was also an exchange of views on the impact that this convention will have on possible cross-border intelligence cooperation between intelligence services and oversight authorities.
- The Canadian oversight authority, NSIRA, presented its risk control matrix for prioritising audit tasks.

IOWG Technical Meeting and Staff Meeting from 23 to 25 October 2024 in Stockholm

At the technical meeting, all participating oversight authorities presented practical examples from their countries on how to deal with large amounts of data. Participants benefited from each other’s experience and expertise, and lively discussions took place.

After presentations on developments in the participating countries, the staff meeting also focused on the handling of large amounts of data, but in contrast to the technical meeting, the staff meeting focused on the non-technical aspects. Each country presented its current legal situation with regard to the oversight of the processing of large amounts of data by intelligence services.

The international meeting in Stockholm clearly showed that all countries are dealing with similar issues, such as an increase in the number of employees in the intelligence services, greater transparency of the intelligence services in the media, and changes in legislation.

8 Appendix

8.1 Audit plan for 2024

No	Title	Audited entity
Strategy and planning		
24-1	Artificial intelligence	FIS
Organisation and tasking		
24-2	Intelligence service activities to be conducted by the Armed Forces Preventive Protection Service (AFPPS)	FIS / MIS & AFPPS
24-3	Organisation of partner service contacts at the CEA (formerly EOC)	FIS / CEA
Cooperation		
24-4	Cooperation between FIS and State Secretariat for Migration (SEM)	FIS
Information gathering		
24-5	Operations / Operational inquiries / Intelligence-gathering measures requiring authorisation	FIS
24-6	Human intelligence (HUMINT)	FIS
Resources		
24-7	ICT Inventory	FIS
24-8	Incident and Risk Management in the MIS	MIS
Data processing and archiving		
24-9	Spot check IASA (ICC)	FIS
24-10	Queries on third-party information systems	FIS

8.2 Abbreviations

AFPPS	Armed Forces Preventive Protection Service
AI	Artificial Intelligence
ArmA	Federal Act of 3 February 1995 on the Armed Forces and the Military Administration (Armed Forces Act, SR 510.10)
Art.	Article
BCM	Business Continuity Management
CAS	Certificate of Advanced Studies
CDel	Control Delegation
CEA	Cyber and Electromagnetic Activities Service
CIS	Cantonal Intelligence Service
DDPS	Federal Department of Defence, Civil Protection and Sport
FAC	Federal Administrative Court
FDPIC	Federal Data Protection and Information Commissioner
FIS	Federal Intelligence Service
FoIA	Federal Act of 17 December 2004 on Freedom of Information in the Administration (Freedom of Information Act, SR 152.3)
FOJ	Federal Office of Justice
GEVER	Business management system
HUMINT	Human Intelligence
IASA-ICC	Information and Analysis System All-Source Integral Control Centre
ICA	Independent Control Authority for Radio and Cable Communications Intelligence
ICT	Information and Communications Technology
IntelSA	Federal Act of 25 September 2015 on the Intelligence Service (Intelligence Service Act, SR 121)
IntelSO	Ordinance of 16 August 2017 on the Intelligence Service (Intelligence Service Ordinance, SR 121.1)
IOWG	Intelligence Oversight Working Group
IT	Information Technology
ITSCM	IT Service Continuity Management
MIS	Military Intelligence Service
NSIRA	National Security and Intelligence Review Agency (Canada)
NW	Canton of Nidwalden
OA-IA	Independent Oversight Authority for Intelligence Activities
OP	Operation
OPI	Operational inquiry
OSINT	Open Source Intelligence
OW	Canton of Obwalden
para.	paragraph
SEM	State Secretariat for Migration
SFAO	Swiss Federal Audit Office
SIGINT	Signal Intelligence
SR	Classified Compilation of Federal Legislation
SA-OAG	Supervisory Authority for the Office of the Attorney General of Switzerland