Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

**Independent Oversight Authority
for Intellgence Activities**

2023 Annual Report

of the Independent Oversight Authority for Intelligence Activities OA-IA

1 Summary

The security situation is changing rapidly, which requires the Independent Oversight Authority for Intelligence Activities (OA-IA) to continually adapt its audit activities. For example, the war in Ukraine and recent developments in the Middle East have influenced the activities of the services under supervision, necessitating a flexible approach by the OA-IA to understanding and auditing these activities.

The transformation of the Federal Intelligence Service (FIS) also required the flexibility and agility of the OA-IA. Furthermore, technological developments such as the use of artificial intelligence (AI) need to be monitored, analysed and incorporated into the OA-IA's audit activities. Adjusting to changing framework conditions is thus a task that also forms a topic of discussion with other oversight authorities internationally.

Looking back on the year, the Audit ‘22-15 Open-source intelligence (OSINT)’ conducted at the Federal Intelligence Service (FIS) proved to be one of the focal points of the OA-IA’s audit activities in 2023. OSINT is a rapidly developing area of information gathering. Linking a seemingly infinite amount of publicly accessible data creates almost endless possibilities for intelligence services to gather information. Legal and ethical questions arise – the distinction between OSINT and information-gathering measures requiring authorisation, for example, or whether the procurement or use of data stolen by third parties still falls within this area. Supervisory authorities around the world are closely observing and discussing intelligence services’ use of this method of information gathering. The OA-IA has audited the FIS’s use of this information-gathering measure and issued various recommendations.

The OA-IA had originally planned to conduct 16 audits in 2023; four of these were cancelled later in the year. One audit from 2021 was completed in 2023. Final reports for seven audits from 2022 were completed and sent off in 2023. Of the audits planned for 2023, the OA-IA completed its audit activities for seven of them and sent three final audit reports to the Federal Department of Defence, Civil Protection and Sport (DDPS).

In addition to the audits completed at the FIS, one audit was conducted on the Electronic Operations Centre (ECO, from 01/01/2024 «Cyber and Electromagnetic Activites Service (CEA)). With regard to the Military Intelligence Service (MIS), the OA-IA conducted various discussions at management level regarding its supervisory authority in the area of the Armed Forces Preventive Protection Service (DPSA) and added an appropriate audit to its audit plan for 2024.

2 Key figures as of 31 December 2023

Staff	01.01.2023	**10**
	31.12.2023	**10**
Planned audits		**16**
Unannounced audits		**0**
Audits conducted		**11**
Number of interviews	oral and written	**109**
Recommendations		**10**

3 Table of contents

4 Personal

A matter of trust

As a lawyer, it’s clear to me that the state can only act as the law requires – and I am confident that if I consult the law, I will understand (nearly) everything about what a particular authority does and why. If I were an engineer, I would be in a better position to understand why it’s still possible to drive through the Gotthard Road tunnel despite the fact that concrete fell from the ceiling last September. As an ordinary citizen, I have to admit that I often have to trust those who know more than I do, such as the Federal Roads Office in my example.

So, with the state, I understand some things on my own, but not others. But there always has to be someone who can explain the state's actions to me. What about the secret services? These services are sometimes accused of being like a "state within a state" because certain activities must not be made public, as if they had a power that no other authority has. As a matter of fact, this power of secrecy is no small matter.

Looking at what the intelligence services actually do, it’s clear that the maintenance of secrecy is used first and foremost as a working tool. If the intelligence services could not use covert means and methods in certain contexts, their actions would be useless.

Of course, as the saying goes, with great power comes great responsibility. Who can guarantee that this right to secrecy will not be abused for fraudulent or selfish purposes such as greed or the pursuit of power?

Swiss legislators have long been aware that this type of power must be subject to robust controls. Parliament’s Control Delegation in particular has been dedicated to the oversight of intelligence service activities since 1992. Legislators successfully expanded their oversight by establishing an independent supervisory authority as part of the new Intelligence Service Act, which was adopted in 2015 and approved by voters in a 2016 referendum.

Nearly all Western democracies have opted for a combined oversight of their intelligence services by a parliamentary body and an independent authority. It provides intelligence services with legitimacy, as they are subject to double oversight. They are thus supervised on the one hand by a parliamentary body representing a wide political spectrum with whom citizens can identify and, on the other hand, by experts such as those I head, who are presenting their work to you in this report.

The intelligence services and the Federal Roads Office have little in common – except that they both rely on trust. The intelligence services need the trust of the public in order to carry out their duties, and the public need the intelligence services in order to benefit from a certain level of security.

The supervision of the authority I head involves monitoring complex and sensitive activities, identifying their risks or failures, as well as making recommendations on how to improve. As a supervisory authority, we cannot disclose all the secrets of the intelligence services, but we can examine and report on them to a certain extent.

In light of all this, the Independent Oversight Authority for Intelligence Activities is pleased to present its annual report – so that every citizen can assess whether they can have confidence.

I hope you enjoy reading the report.

Prisca Fischer, Head of OA-IA

5 Oversight activities

5.1 Audit plan

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

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

The Audit plan is designed to include at least one audit from every audit area. The audit plan that had been published for 2023 was changed during the year, as four audits were cancelled for the following reasons:

- '23-1 Generation and impact of intelligence products (FIS)'. The FIS is currently undergoing a transformation. Changes can be therefore expected in its production activities, in addition to changes to its organisational structures.

- '23-3 Protection and security (FIS)'. This audit was cancelled in order to give priority to others, as previous audits have examined certain security-related aspects. Audit '22-14 Recruiting, support and leaving processes', for example, looked at security for staff members. Staff security remains a focus issue for the OA-IA.

- '23-14 Implementation of OA-IA recommendations'. The OA-IA launched an internal project aimed at improving the quality of its recommendations. Two staff members attended a continuing education course and wrote a transfer paper on this topic. The OA-IA will update the audit handbook based on the results and also intensify its monitoring of recommendations. In light of the new situation, this audit has been put aside in order to give others priority.

- '23-15 Compliance with the right to receive information'. The Federal Act on Data Protection was amended on 1 September 2023 (Data Protection Act, FADP; SR 235.1). The FIS requires sufficient time to implement the required changes into its procedures. The OA-IA maintains a dialogue on this issue with the FIS and the Federal Data Protection and Information Commissioner (FDPIC).

5.2 Audits conducted in 2023

Starting with this year's report, the OA-IA is changing the format of its reporting. Previous reports provided information only on audits that had been completed during the year under review. This and future reports will provide information on all audits that were worked on during the year, including audits that had begun in prior years or those that were not yet formally completed in the year under review.

5.2.1 Strategy and planning

In the area of 'Strategy and Planning' the OA-IA checks issues that relate to the short-, medium- or long-term strategic planning of Swiss intelligence services and their objectives. It carried out the following audit in the year under review:

22-1 Anticipation and early detection

This audit focused on the issue of how the FIS can best carry out its legal mandate of early detection and anticipation. The FIS's information gathering and processing activities facilitate the early detection and prevention of threats to internal and external security. It must therefore be capable of identifying and assessing a situation at an early stage. The growing complexity of international geopolitical systems is leading to a drastic increase in uncertainty with respect to the future development of threats. **Social and technical advances as well as the hybrid and global nature of today's threats**

require the FIS to detect these threats and to respond to them quickly and effectively. The anticipation and early detection of relevant threats, strategic developments and corresponding opportunities are vitally important in this context, and the FIS plays an important role for its clients in the early detection of threats and crises.

The OA-IA audit showed that anticipation and early detection are among the strategic objectives that the FIS has been working towards for some time, and for which it has already implemented operational measures. Some of these measures are well advanced, while others must be intensified. The OA-IA found that the topic is broadly supported with the necessary importance at the strategic level. The prioritisation of early detection and anticipation in the respective strategies of the DDPS and the FIS, and the statements of staff members who work in this field, show that this topic is hugely important.

However, the OA-IA also noted that the (theoretical) considerations of the FIS are only very slowly flowing into the evaluating areas of the service. The link between the available instruments and the resulting products must be improved, which would make the FIS more successful in transforming its conceptual efforts into value-adding products. The OA-IA therefore issued a recommendation that the FIS consistently pursue the individual implementation measures for early detection and anticipation as set out in the FIS Strategy 2020–2025 and review the implementation status at least once a year.

The OA-IA expects that the FIS will use its current transformation to create an agile, innovative and adaptable service, bearing in mind that a reorganisation alone will not accomplish this. Management, in particular the FIS upper management, must work continually see that the service is kept up to date in terms of structure, innovative working methods and new technologies in order to be able to react promptly and adequately to changing threats.

5.2.2 Organisation

In the area of ‘Organisation’ the OA-IA checks the suitability of the structure and processes of the intelligence services and asks whether they enable the authorities to carry out their legal mandate in a lawful, expedient and effective manner. The OA-IA conducted the following audits in this area in 2023:

23-2 Legal services at the FIS

In intelligence service activities, compliance with the law holds great importance. If the FIS does not act lawfully, i.e. within the scope of its legal mandate, this will damage its reputation as well as the trust the Swiss population places in it. Personal rights in accordance with data protection regulations, the right to privacy or business secrecy may also be violated. On the other hand, there is a considerable security risk for Switzerland if legal uncertainty prevents the FIS from fully exploiting its possibilities within the framework of the law and it therefore fails to fulfil its mandate.

Against this background, the OA-IA examined the expediency and effectiveness of the tasks, competencies and responsibilities of those providing legal services. In this review, legal services were defined as FIS activities that included answering a specific question, providing general information on the legal background, legislative projects and court rulings, asserting disputed and undisputed claims and participating in projects and the conclusion of contracts. The OA-IA did not review the quality (legality) of the legal services provided.

The OA-IA conducted eight interviews, mainly with managers, and provided 30 staff members with a questionnaire to gather opinions on the services provided. It also analysed and evaluated documentation relating to tasks, responsibilities and legal services in the FIS records management system.

The audit began in 2023, and the report had not yet been completed at the time this annual report was being drafted. For this reason, no assessment could be made at that time. The OA-IA will publish the audit summary on its website once it has been completed.

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

In this audit, the OA-IA examined whether the FIS has efficient and appropriate procedures in place to handle emergencies in IT operations, and thus whether the critical business processes of the FIS can be guaranteed and its data can be restored.

Major unforeseen incidents such as fires, floods and criminal activity pose a threat to every organisation, and they can cause damage – particularly to IT infrastructure – with far worse consequences than a simple malfunction. Organisations must therefore ensure business continuity management (BCM), which analyses the risks posed by an incident and aims to minimise their impact on critical services and business processes.

Given the heavy reliance of business operations on information technology, the existence of a fail-safe IT infrastructure is essential for the survival of an organisation. ITSCM along with BCM ensures that even when major incidents occur, the IT services that the organisation has identified as critical can be delivered. To this end, precautionary measures (strengthening resilience) and measures developed for use in the event of an incident (strengthening the response) are assessed and implemented. ITSCM must ensure that services and infrastructure relating to information and communications technology (ICT) are available after a failure or can be restored within an agreed period of time. IT Disaster Recovery, on the other hand, is intended to restore ICT services and infrastructure after a failure.

Effective ITSCM must take into account the current and specific risks. **Given advancing digitalisation and the status of data processing as the FIS's central activity – and against the backdrop of potential power 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 jeopardises the FIS's ability to fulfil its mandate.

BCM was already the subject of a report by DDPS Internal Audit (Report I 2022-01 of 15 August 2022). One of the recommendations in the report called on DDPS administrative units to update their BCM documentation. The FIS is working on implementing 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 more reserved approach to BCM issues.

The OA-IA found that certain ITSCM documentation was lacking due to insufficient IT governance within the FIS. Measures have been taken in this area, but only at a technical level. The FIS's ICT unit has taken numerous measures to ensure business continuity in the event of a major incident. The planned measures are efficient and appropriate for the situation; they include, in particular, ensuring the redundancy of the ICT infrastructure and the data security strategy, and enabling risks to be minimised. However, there is no testing strategy, so it is not certain whether ICT service provision would actually maintain its high level of stability in the event of a major incident. Furthermore, the ITSCM plan cannot be updated without multifaceted and regular testing. Recommendations were made in connection with ITSCM documentation and the organisation of testing.

5.2.3 Cooperation

The OA-IA checks the level of cooperation between the cantonal intelligence services and national and international authorities. Each year, the OA-IA examines cooperation with selected cantonal intelligence services (CISs). The kick-off meeting for audits'23-6 KND N' and '23-7 KND OW' was still held in 2023, with further audit activities carried out in 2024. The OA-IA will publish the summaries of the audits on its website once they have been completed.

In 2023, it conducted the following audits:

23-5 Cantonal Intelligence Service of Lucerne

The OA-IA examined whether cooperation between the FIS and CIS Lucerne was legal, expedient and effective, and came to the conclusion that the two services had a close working relationship and

worked together well or very well in a number of fields. CIS Lucerne completed the mandates given to them by the FIS on time and according to the mandate issued. The OA-IA audit found that CIS Lucerne has a very good network, has good intelligence information as well as the necessary conditions and motivation needed to accomplish intelligence tasks.

In particular, the OA-IA checked whether the personal data that was stored and recorded complied with the legal requirements in terms of task reference, compliance with data processing restrictions and the accuracy and relevance of the information. It found no serious anomalies in this regard, but nevertheless suggested that a systematic check be carried out in all files.

23-8 Cantonal Intelligence Service of Uri

The OA-IA examined whether cooperation between the FIS and CIS Uri was lawful, expedient and effective, and came to the conclusion that the two services had a close working relationship and worked together well in a number of fields. CIS Uri completed the mandates given to them by the FIS on time and according to the mandate issues. The OA-IA gained the impression that CIS Uri has good intelligence information and the qualities necessary for its work. It also has the necessary conditions and motivation needed to accomplish the tasks assigned to it.

In particular, the OA-IA checked whether the general and personal data that was recorded complied with legislative provisions in terms of task reference, compliance with data processing restrictions and the accuracy and relevance of the information. It found no anomalies in this regard.

23-9 Technical sensor mandates at the Electronic Operations Centre (EOC, from 01/01/2024 **‘**Cyber and Electromagnetic Activites Service (CEA)**’.)**

Technical sensors are an important tool for gathering intelligence information. The technology underlying information gathering is constantly evolving, and technological development potentially enhances the effectiveness of this activity. Organisations active in this area must therefore remain mindful of how to develop their capabilities in the acquisition of intelligence-relevant information, but risks can arise if the relevant legal framework is not given the necessary priority in these considerations.

Against this background, the OA-IA reviewed the CEA’s use of technical sensors for FIS assignments. It found that the CEA always requires a detailed written mandate for intelligence service-related assignments. Traceability, compliance with legal deadlines and the allocation of results to the original assignment are ensured at all times by storing mandates in a central administrative mandate management system.

In its operational activities, the CEA seeks ways to use intelligent tools in order to relieve scarce human resources of routine activities while at the same time making better use of the data obtained from radio and cable reconnaissance, particularly with regard to future cyber threats.

With regard to compliance with the legal basis in operations, the OA-IA found that CEA staff are regularly reminded of the relevance of the legal basis for their day-to-day business, and that there are also organisational measures in place, such as internal peer reviews of results and directives issued by CEA management.

Overall, the OA-IA found no indication that the CEA’s use of technical sensors to carry out intelligence-related mandates violates the legal basis, or that the sensors are not used effectively or expediently.

23-10 FIS cooperation with private actors

The FIS conducts its information gathering activities partly covertly. This is essential because if the affected states and actors become aware of these activities, they can take countermeasures. In addition, covert activities protect FIS staff, facilities and intelligence sources.

Effective cover stories must be established and maintained in order to conceal an individual's FIS affiliation or activities. To do this, the FIS requires the assistance of private actors to accomplish this, among others. For the purposes of this audit, the term 'private actors' was used to refer to anything that is not a domestic or foreign administrative unit.

According to the Federal Act on the Intelligence Service (Intelligence Service Act, IntelSA; SR 121), the FIS may cooperate with private individuals, companies and organisations. These can provide services for the FIS that serve the fulfilment of its mandate in accordance with the IntelSA or they can support the FIS in information gathering. The FIS may also issue information-gathering mandates to private actors if this is necessary for technical reasons or because of access to the information source. This gives rise to a number of issues regarding the legality of the assignment and the organisation. These include the circumvention of information-gathering measures generally requiring authorisation, unlawful conduct by private actors, payments without consideration and cooperation with persons of dubious reputation. What is needed is an overview of the private actors deployed and their recruitment, security clearance, compensation, documentation and so on.

Careless actions, particular those taken by private actors, can allow third parties to draw undesired conclusions about FIS staff and facilities as well as about the sources, thereby putting them at risk. Private actors employed by the FIS may also, whether knowingly or unknowingly, behave unlawfully in the course of their work for the FIS. If these risks were to occur, it would not only have operational consequences – such as hindering or even preventing information gathering – it would also inevitably damage the reputation and credibility of the FIS.

The OA-IA therefore examines whether the FIS's cooperation with and commissioning of private actors is legal. It also examines whether the private actors commissioned by the FIS are systematically checked in terms of risks and benefits, and whether the cooperation and commissioning of private actors is organised effectively and expediently and coordinated and documented in a plausible and conclusive manner.

This audit began in September 2023 and was still ongoing as this activity report was completed. It is therefore not yet possible to make any statement about the audit results. The OA-IA plans to publish the summary of the audit on its website in 2024.

5.2.4 Information gathering

Information gathering is a core task of intelligence services. Various means can be used for this purpose. The OA-IA pays special attention to those that most deeply invade the privacy of the persons concerned. In the area of 'information gathering', the OA-IA conducted the following audits in 2023:

22-10 Information management using information-gathering measures not requiring authorisation

The FIS can take certain information-gathering measures not requiring authorisation independently and without having to obtain specific external authorisation. This is true in cases where the intensity of interference with fundamental rights is relatively low. If this type of information-gathering measure cannot secure the essential information required to ensure Switzerland's security, the FIS can employ measures that interfere more strongly with the fundamental rights of the persons involved and therefore require authorisation. The required level of monitoring increases in proportion to the level of interference with fundamental rights. Information-gathering measures requiring authorisation must therefore first be authorised by the Federal Administrative Court (FAC) and then given clearance by the head of the DDPS in consultation with the Federal Council Security Committee. Only then can the FIS implement the measures. Measures that do not require authorisation, and thus are not subject to external review, are open to the risk of being carried out unlawfully, for example if they impact processes or facilities that are considered to belong to the private sphere.

The OA-IA therefore examined whether the FIS uses procurement measures not requiring authorisation lawfully. It found that the FIS generally has practicable resources and the required capabilities to deploy such measures proportionately and appropriately in accordance with Articles 14 and 16 of the IntelSA.

It also found that the process the FIS has established for initiating information-gathering measures not requiring authorisation creates the necessary conditions for the lawful implementation of these measures in accordance with Articles 14 and 16 IntelSA. In principle, the FIS makes lawful use of information-gathering measures not requiring authorisation.

No matter which information-gathering measures are used, the information obtained is useless if it cannot be evaluated effectively and expediently. To analyse videos, for example, the FIS therefore relies on electronic support in the form of analysis software. In this specific case, the OA-IA concludes that it is lawful to use analysis software to assist with video evaluation.

With regard to the use of the computerised police search system (RIPOL) and the national part of the Schengen Information System (N-SIS), the OA-IA examined the processes for issuing alerts as well as the access authorisations and data queries carried out from the two systems. The OA-IA found that the process of issuing alerts in RIPOL and N-SIS is fundamentally lawful. However, it also found that not all of the FIS's RIPOL and N-SIS queries are documented in such a way that it is clear whether they were justified for official purposes. The OA-IA therefore issued a recommendation that the FIS carries out regular monitoring checks on the RIPOL and NSIS searches by FIS staff and documents the monitoring checks.

The FIS has the option to use forms of information-gathering measures which always require authorisation from the FAC in accordance with Article 26 IntelSA and clearance in accordance with Article 30 IntelSA, for example special technical equipment for monitoring telecommunications, tracking devices or locking and opening technology. Although measures of this nature require authorisation and clearance, it would be possible for the FIS to use them without the knowledge of the authorities provided for in the IntelSA and therefore without the required approval. In the course of its audit procedures, the OA-IA found no evidence that the FIS uses the information-gathering measures listed in Article 26 IntelSA without the necessary authorisation and clearance.

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

Intelligence service operations (OPs) and operational clarifications (OPCs) are among the FIS's core tasks. They are more complex than day-to-day business and require operational management. In addition, information-gathering measures requiring authorisation can also be requested in OPs. The OA-IA regularly examines OPs, OPCs and information-gathering measures requiring authorisation because of the complexity of OPs and OPCs regularly entails risks relating to effectiveness and expediency, while measures requiring authorisation always involve a legal risk due to their interference in the private sphere.

In its annual audit, the OA-IA analysed the legality, expediency and effectiveness of five selected OPs and 13 OPCs. In addition, 12 authorised and cleared information-gathering measures were examined to determine whether their implementation complied with the decisions of the FAC. The audit procedures included documentation reviews and interviews with the experts responsible.

The audit began in 2023 and had not yet been completed at the time this annual report was finalised. The OA-IA published the summary of the results of this audit on its website at the beginning of 2024.

23-12 Human intelligence (HUMINT) in the FIS

In order to fulfil its tasks, the FIS obtains information from publicly and non-publicly accessible information sources. Some of the information-gathering measures it uses for this purpose require authorisation while others do not. Obtaining information from human sources is an information-gathering measure not requiring authorisation. Human sources are individuals who provide information or intelligence to the FIS, provide services for the FIS that serve to fulfil its legal mandate, or assist the FIS in obtaining information. HUMINT (the use of human sources) is often associated with high personal risks for both FIS staff and their sources. This entails a special responsibility and

obligation on the part of the FIS, which it must take seriously. It is therefore also given due importance in the OA-IA supervision.

The OA-IA examined how the FIS actually manages its source portfolio and how the portfolio is developing. It used random sampling to verify the legality, expediency and effectiveness of source management. Particular secrecy is required in this area in order to protect sources and personal safety; the OA-IA's HUMINT audits are therefore given the classification level 'secret'.

This audit began in August 2023 and had not been completed at the time this annual report was finalised. For this reason, no statement can be made yet about its results. The OA-IA will publish the audit summary on its website in 2024.

5.2.5 Resources

In the area of 'Resources', the OA-IA considers whether the intelligence services are handling resources in an expedient manner and whether intelligence activities are carried out effectively. In 2023, the OA-IA conducted the following audits relating to 'Resources':

22-13 Legended financial flows

The OA-IA examined whether the FIS has lawful, expedient and effective ways to make financial payments without being identified as the remunerator. It also examined whether the funds transferred in this way are used exclusively for the fulfilment of tasks in accordance with Article 6 IntelSA.

The OA-IA found that the FIS has various proven and ready methods at its disposal to transfer funds to recipients without being identifiable as the remunerator.

The FIS refers to individuals who assist with legended financial flows as supporters and classifies them as 'human sources'. IntelSA also defines individuals who support the FIS in its activities and provide it with services that serve to fulfil its legal mandate as 'human sources'. The OA-IA shares this view and therefore recommends that the FIS aligns the management of supporters more closely with the management of 'human sources in the narrower sense' and establishes binding regulations. Such regulations include, in particular, a systematic and well-founded examination of the risks, benefits, potential and costs of each supporter. In addition, supporters are to be listed in summary form as 'human sources' in the annual reporting in accordance with Article 19 of the Federal Ordinance of 16 August 2017 on the Intelligence Service (Intelligence Service Ordinance; SR 121.1).

In order to enforce the IntelSA, the FIS may cooperate with foreign intelligence services by carrying out joint activities to obtain and evaluate information and assess the threat situation. In two specific cases where the FIS engaged in joint activities with foreign partner services, the OA-IA found that although the FIS did consider the legality, associated (reputational) risk and expected benefits of the cooperation, it did not document these considerations sufficiently. The OA-IA therefore encourages the FIS to pay more attention in future to careful and detailed documentation of such considerations and the resulting decisions.

22-14 Recruiting, support and leaving process

The FIS can face security risks from its own staff members, who may betray the organisation, steal data or engage in espionage. Dissatisfied employees are also potentially more likely to leave the service, which can lead to staff turnover-related challenges. Valuable know-how can be lost and resources expended on recruiting new members of staff.

The OA-IA believes that these risks have increased in the FIS in recent years. This assessment is confirmed by the significant increase in reports and information about dissatisfied FIS employees, frequent changes at the top-management level, the results of the 2020 Federal Administration staff survey and the high staff turnover rate at the FIS more generally.

The OA-IA conducted a large number of interviews with staff members and a random sampling of personnel files. These audit activities took place from July to mid-November 2022. At the time of the audit, the FIS was in the process of preparing and implementing its transformation, during which it was decided to revise important documents and processes relating to staff recruitment, support and leaving. The OA-IA paid special attention to this state of organisational development in its audit report. In summary, it found that the FIS had formulated the right objectives in its personnel strategy. These were also reflected in the objectives of the transformation.

It found that there were some serious shortcomings in the FIS's personnel administration and management. These concerned the documentation in personnel files, the way that annual performance reviews and staff appraisals were conducted and the clarification procedure regarding employees in particularly critical situations. The OA-IA issued various recommendations in this regard.

In particular, the resources of the support units in the FIS, such as Human Resources, must be increased so that the tasks associated with staff recruitment, support and departure can be executed correctly. This is currently all the more important so that the FIS can realise the transformation process correctly.

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 due to the fact that the information processed by intelligence services is highly sensitive and the legal requirements are as extensive as they are complex. In 2023, the OA-IA conducted the following audits in this area:

21-16 Telecommunication services

The OA-IA examined whether information provided by the FIS on services from selected telecommunication providers is legal and expedient. The FIS receives requests for access to information on providers of derived communication services (PDCS), and in particular to secondary telecommunication data from end-to-end encryption applications from Swiss providers. In the past, the FIS has noted an increase in such requests.

The audit focuses on PDCSs that operate platforms in Switzerland and are therefore subject to the provisions of the Swiss Telecommunications Act (TCA; SR 784.10). Based on IntelSA[1], the FIS can obtain information in accordance with the Federal Act on the Surveillance of Post and Telecommunications (SPTA, SR 780.1). For the purpose of fulfilling tasks under the IntelSA, the Post and Telecommunications Surveillance Service (PTSS) of the Federal Department of Justice and Police provides the FIS with information on the data upon request[2].

With regard to end-to-end encryption applications, the law allows the FIS to obtain information from the PTSS without authorisation or to carry out monitoring that requires authorisation.

The audit revealed that the FIS only processed requests that were related to its core mission. The OA-IA considered the process for the centralised processing of requests to be appropriate. The FIS had not always fully documented the requests that the OA-IA examined. In one case in which the FIS was gathering information lawfully, it also processed additional information which it had received without requesting it and, in this case, without a valid legal basis. In both cases, the OA-IA issued a recommendation.

22-15 Open-source intelligence (OSINT)

Open-Source Intelligence (OSINT) is a rapidly developing area of intelligence gathering. Collating seemingly infinite amounts of open-source information (OSINF) creates almost endless possibilities for intelligence services to generate intelligence. The analysis of this OSINF, with the aim of obtaining

[1] Art. 25 para. 2 IntelSA

[2] Art. 21 and 22 SPTA

useful information from it, is referred to as OSINT. What is more, gathering OSINF 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 gives rise to legal and ethical questions, such as where to draw the distinction between OSINT and HUMINT, particularly with regard to the use of alias identities online for person of interest investigations or to obtain data records offered illegally on the internet (leaks). The OA-IA therefore decided to examine the FIS's use of OSINT.

In accordance with Article 13 IntelSA, public sources of information include, in particular, 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 discussed by the FIS's partner services and foreign supervisory authorities. If there is no uniform understanding of these boundaries, there is a risk of unlawful information gathering. The interviews conducted with employees from the FIS's OSINT unit 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. The use of various information-gathering measures in the area of OSINT is therefore not clearly and uniformly regulated in the FIS. The OA-IA issued a recommendation to define the legal framework for gathering OSINT-related information and uniform regulations for using OSINT.

The OA-IA examined selected cases of OSINT-related information gathering and found no indications of unlawful activity. In accordance with Article 22 paragraph 1 of the Government and Administration Organisation Ordinance (GAOO, SR 172.010.1) in conjunction with Article 52 IntelSA, the FIS is obliged to provide evidence of its own activities by means of systematic records management. Based on Article 2 of the Ordinance on Electronic Records and Process Management in the Federal Administration (GEVER Ordinance, SR 172.010.441), the Directive of 7 July 2022 on the Filing and Archiving of Documents in the FIS also stipulates in chapter 2 that all business-relevant documents must be registered and filed in GEVER FIS. The OA-IA found that some cases of OSINT-related information gathering were insufficiently documented and did not comply with the applicable Federal Administration regulations, which made it impossible for the OA-IA to assess its legality. The OA-IA issued a recommendation in this case.

OSINT tools are used to generate intelligence-relevant information expediently and effectively from the huge amount of data available through publicly accessible sources online. The FIS employs a mix of standard commercially available products and in-house developments that enable the use of online alias identities (OAIs) for permanent monitoring and targeted searches. OAIs exhibit anomalies due to their use by intelligence services and could therefore be classified as potential targets by other agencies and become the focus of partner services. To counter this risk, the OA-IA proposed transferring the FIS OAIs to the existing international database and ensuring that the FIS and the CISs are mutually informed about the OAIs they are deploying.

The FIS uses a special IT infrastructure for anonymised OSINT-related information gathering. This infrastructure has security vulnerabilities and should be upgraded or replaced in the near future. The OA-IA issued a corresponding recommendation.

It can be difficult to verify findings from OSINT research, especially in the case of information generated from the darknet. The FIS sees it as integral to intelligence service activity to treat information with an appropriate degree of suspicion. If information cannot be verified or its veracity cannot be quantified, this is indicated in the OSINT reports. Source verification, which plays an important role in the detection and disclosure of fake news, for example, is a particularly well-known problem when using complex commercially available OSINT products and is also a recurring theme within the intelligence community.

In addition to the FIS, CISs also carry out OSINT research. The OA-IA examined possible duplications and inefficiencies. It came to the conclusion that the agencies are aware of the risks and are taking

action to counter them, for example by ensuring regular discussion of OSINT in a recently created forum.

The content of the OSINT information system (OSINT Portal), which contains research results and raw material from open sources, is governed by Article 54 paragraph 2 IntelSA and Article 46 ff. of the Ordinance on the Federal Intelligence Service Information and Storage Systems (ISSO-FIS, SR 121.2). The FIS uses the information system to make data from publicly accessible sources available internally. The audit procedures, and in particular random sampling, did not provide the OA-IA with any indication that the OSINT portal violates the expediency or effectiveness of data management. OSINT data has a shorter retention period than data generated using other sensors. This eliminates the risk that sensor mislabelling could lead to an unlawful extension of the data retention period for OSINT data.

22-17 Follow-up to 20-19: Archives of the FIS

Audit 22-17 is the follow-up to Audit '20-19 Archives'. It was organised following media reports of FIS 'secret archives' in connection with the Crypto AG case. In the 20-19 audit, the OA-IA found that analogue documents classified as SECRET were stored in a location also classified as SECRET. At that time, the FIS and the Swiss Federal Archives (SFA) were discussing the transfer of documents for archiving purposes, and some of these documents had also been mentioned in the media. These materials mainly concerned pre-2010 documents from the FIS's predecessor organisations. The OA-IA accordingly refrained from issuing recommendations and announced a follow-up audit.

In addition to reputational risks, in Audit 22-17 the OA-IA examined risks relating to the legality, expediency and effectiveness of the archiving and retention of documents. In the case of archiving, the aim was to clarify whether the documents were offered and delivered to the SFA lawfully and in accordance with the agreement, and whether documents were withdrawn or destroyed before or after they were offered to the SFA, or after they had been granted archival value by the SFA. With regard to document retention, the audit was intended to examine whether retained documents should have been archived and whether this process was in compliance with retention standards.

During Audit 22-17, the OA-IA inspected the local document storage locations and carried out random sampling. It found that the work of archiving analogue documents (mainly paper documents and microfiches) is well advanced at the various locations where the FIS stores documents. Overall, the OA-IA notes that the situation has improved, and that the commitments made during the 20-19 Audit (mainly concerning the implementation of the agreement with the SFA) have been met. The work carried out is in line with the agreement between the FIS and the SFA. Where submission deadlines could not be met, there were comprehensible, credible reasons only partially attributable to the FIS. Several thousand documents (almost 200 linear metres) and millions of microfiches, mainly relating to the predecessor organisations of the FIS, were inventoried and delivered to the SFA. The materials delivered cover the period from 1938 to 2021.

As the documents of the predecessor organisations were not inventoried, it was not possible for the OA-IA to investigate the risks it had identified, in particular whether all documents were actually offered and delivered to the SFA or whether some documents were destroyed, whether accidentally or intentionally. The OA-IA found no evidence that these risks had materialised.

The work of reviewing and archiving the documents is still ongoing. In this respect, the agreement has not yet been fully implemented. The FIS was requested to remedy this. The OA-IA found that the documents held have not been inventoried, and it therefore issued a recommendation that the FIS inventory the documents that it will retain (i.e. those that will not be delivered to the SFA).

22-18 Data collection by Cyber FIS

The unlawful data collection by Cyber FIS, which has been the subject of various media reports, was investigated both internally by the FIS itself and in an externally led administrative investigation. The OA-IA initiated its own investigation because it found that both reports left certain questions

unanswered. Analysing the extensive data collections involved, which had not yet been viewed or evaluated either by the FIS itself or as part of the administrative investigation, proved to be challenging and time-consuming. The audit was still in progress at the editorial deadline for this annual report and therefore no statement can be made at this time about the audit results. The OA-IA plans to publish the audit report on its website in 2024.

23-16 Information systems, storage systems and data repositories not listed in Article 47 IntelSA

The IntelSA regulates data processing. Article 47 IntelSA provides a list of information systems operated by the FIS; whether this list is exhaustive was a topic for discussion when the new Intelligence Service Act was being drafted. The OA-IA wanted to clarify this legal question and evaluate which other systems are used for which purposes. The associated legal bases were also analysed in order to determine whether they were sufficient.

This audit began in August 2023 and had not yet been completed as of the editorial deadline for this annual report. For this reason, no further statements can be made about the results of the audit at this time. The OA-IA plans to publish the audit report on its website in 2024.

Clarification of cyberattack on Xplain AG

Due to the cyberattack on Xplain AG, the OA-IA carried out a clarification procedure beyond its usual annual audit planning. The focus was on whether and to what extent the attack also involved FIS data and how the FIS dealt with the incident as part of its basic mandate. The findings from the investigation were partially incorporated into Audit ‘23-10 Cooperation with private parties’.

5.3 Acceptance

The OA-IA auditors were welcomed by the audited organisation units in a constructive and professional manner. They were given direct access to the documents and information systems required to carry out their audit tasks. Auditors also had no difficulty reaching interviewees whenever they needed them. Any further questions were answered as quickly as possible.

5.4 Controlling implementation of recommendations

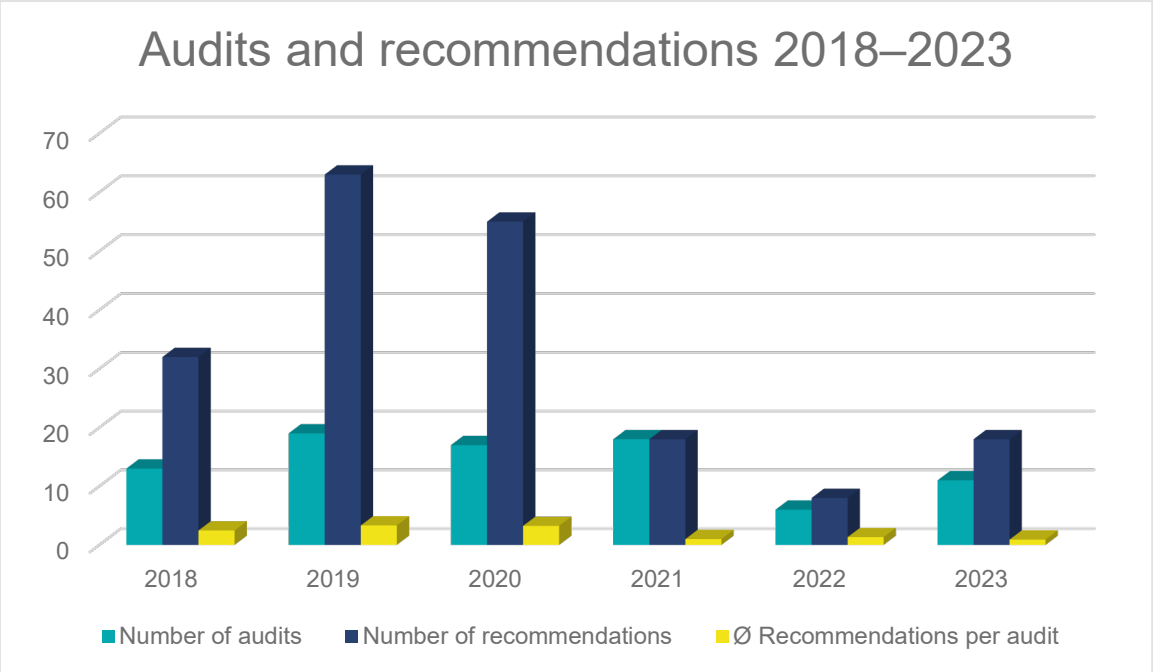
The OA-IA can issue recommendations on the basis of its audit activities and submit these to the head of the DDPS. The DDPS then ensures that these recommendations are implemented. If the DDPS were to reject a recommendation, it would have to submit it to the Federal Council for a decision. No recommendations have been rejected up to this point.

The legal basis stipulates that the OA-IA issues recommendations and the DDPS implements them. Although the legal bases of the intelligence service allow for the OA-IA to issue a recommendation, they do not contain any statements regarding the quality of implementation or controlling activities.

However, effective and credible oversight is only possible if the recommendations made are implemented on the one hand and if correct implementation is also checked on the other. Together with the audited services and the DDPS, the OA-IA is constantly refining this complex aspect of supervision.

The following chart shows the ratio over the last six years of the number of audits carried out versus the number of resulting recommendations. After a three-year initial phase during which an average of two to three recommendations were issued per audit, in the last three years only around one recommendation per audit has been issued on average. The OA-IA's consistent approach of providing a concrete benefit for risk reduction or elimination with its recommendations is therefore reflected in the figures. The result has been fewer, but more targeted and effective recommendations. The number of recommendations does not provide any indication of improvements or deteriorations in conditions, as no audit has been repeated one-to-one to date.

	2018	2019	2020	2021	2022	2023
Number of completed audits by year	13	19	17	18	6	11[3]
Number of recommendations	32	63	55	18	8	10
⌀ Recommendations per audit	2.46	3.32	3.24	1.00	1.33	0.91



6 Insights from the inside

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

6.1 Personnel

In 2023, the OA-IA – as budgeted – set a target of ten staff members. There were two departures from the OA-IA in 2023, while two new members of staff were welcomed during the year.

6.2 Initial and continuing training

Data science training from armasuisse

This year, the OA-IA once again took advantage of the opportunity offered by armasuisse to learn more about the status of current research projects. As in the previous year, the OA-IA focused on the data science research programme. While last year's speakers focused on how to determine the authenticity of image and media content, this year's symposium dealt with the use of artificial intelligence and AI-supported tools in data analysis, as AI is developing at a tremendous pace. Today, AI is able to take data and extract information that can be used to generate knowledge – for example, AI tools are used to recognise patterns and repetitions in data sets. The aim of armasuisse's current research is to develop AI that can use this knowledge to make reliable statements about the future. An understanding

[3] 21-16 (2) / 22-1 (1) / 22-5 (0) / 22-8 (0) / 22-10 (1) / 22-13 (1) / 22-14 (4) / 22-17 (1) / 23-5 (0) / 23-8 (0) / 23-9 (0).

of correlation and spurious correlation of data plays an important role here, as do the methods that can be used to ensure the robustness of the reasoning used.

Further training on conducting audits

Two OA-IA staff members attended a training course on conducting audits offered by the Federal Administration Training Centre. They chose this training course because it covered best practices in the auditing field, refreshed certain skills and allowed them to compare their own practice with that of other Federal Administration offices that conduct audits.

The training course covered the various steps of an audit, from preparation to finalisation, as well as the role of an auditor and the principles of auditing. Course participants could compare their experiences in various group exercises. Finally, the formulation of recommendations and conclusions during an audit was also covered.

The latter was of particular value for OA-IA staff, as there are currently internal discussions regarding the formulation of recommendations and how to make improvements in this area. OA-IA course participants were able to explore the topic in detail as part of a transfer project. The conclusion of the transfer work was that recommendations must be comprehensively formulated but give the audited service room for manoeuvre. Well-formulated recommendations defining what risk must be minimised help the audited service to understand and accept the recommendation and take responsibility for implementing it. The document drafted by the course participants will serve as a basis for reflection in future to enable targeted optimisation within the OA-IA.

Certificate of Advanced Studies (CAS) ‘Digital Forensics and Cyber Investigation Fundamentals’

In the year under review, one OA-IA staff member completed a CAS Digital Forensics Fundamentals. The course consisted of four block modules: digital forensics fundamentals, cyber investigation fundamentals, cybercrime overview and digital forensics acquisition. The knowledge gained from the course flowed directly into Audit 22-18 and the associated data analysis. For example, a method employed in digital forensics was used to analyse an extensive data set.

CAS ‘Communication’

The OA-IA creates its own website content in addition to compiling and publishing the annual report. In order to deepen their technical expertise in communication, one staff member is working towards a CAS Communication, which she will complete in 2024.

Information Systems Audit and Control Association (ISACA) Europe Conference: ‘Digital Trust World’, 18–19 October 2023, Dublin

The ISACA is an independent professional association for auditors, IT auditors and professionals working in the fields of IT governance and information security. A member of OA-IA staff who holds ISACA certification as an IT auditor took part in the association’s annual two-day European conference.

Various presentations on current topics relating to a secure and trustworthy digital ecosystem offered the opportunity to enhance expertise and discuss findings, trends and best practices. The focus was also on the influence that AI and machine learning could have on the security situation, and also on auditing activities in the cyber sector. The findings were incorporated into the OA-IA’s own risk management and audit activities.

Federal Data Protection and Information Commissioner (FDPIC) event on data protection, 17 August 2023, Fribourg (Switzerland)

In view of the entry into force of the new Data Protection Act (FADP), the FDPIC held an information event for data protection officers working in the federal government. Two OA-IA staff members participated in the event, where they also met with staff from the audited units.

The FDPIC and his staff, as well as representatives of the National Cyber Security Centre and the Federal Office of Police, presented topics relating to the amendments to the FADP. These included data protection impact assessments, the use of the new register of processing activities, the FDPIC's new powers to investigate breaches of data protection regulations, logging and more. This successful event featured instructive presentations that will be useful both in the OA-IA's administrative activities and in the context of supervisory activities.

6.3 The audit of the OA-IA by the Swiss Federal Audit Office (SFAO)

The SFAO is the supreme financial supervisory body of the Swiss Confederation, and is independent and autonomous within the scope of legal and constitutional provisions. The OA-IA's institutional independence is likewise enshrined in law.

The SFAO carries out financial supervision according to the criteria of regularity, legality and economic efficiency. Its tasks include examining internal control systems and using spot checks to examine the payment orders issued by the administrative units. It is responsible for auditing the administrative units, including accounting and holdings. The OA-IA does not conduct its audits according to the same criteria. Its legal mandate is clearly differentiated from that of the SFAO.

In its 2023 annual audit programme, the SFAO announced that it would audit the OA-IA. The audit took place from 14 August to 1 September 2023. Its aim was to assess the effectiveness and expediency of the OA-IA's supervision of intelligence activities. On 12 June 2023 the SFAO presented the OA-IA with the audit questions:

1. Does the OA-IA's supervision of intelligence activities comply with the legal basis?
2. Does the OA-IA have sufficient resources for adequate supervision of all actors in intelligence activities?
3. Does the IT infrastructure enable supervision to be carried out efficiently?

In spring 2023 the OA-IA provided the SFAO with six complete audit dossiers from 2021 and 2022 selected at random along with other documents such as concepts and manuals. The SFAO conducted numerous interviews with OA-IA staff, employees of the various audited bodies and the General Secretariat of the DDPS.

In their assessment, the SFAO auditors faced the challenge of not comparing the two authorities (SFAO and OA-IA) too closely. **From the OA-IA's perspective, it was important for the SFAO to understand that the OA-IA performs a different oversight activity and therefore does not function in the same way as the SFAO**. These fundamental differences were discussed again in the final meeting in order to reconcile the two authorities' respective powers. The SFAO continues to carry out its supervision according to its own criteria; the creation of the OA-IA has not changed anything with respect to its scope of responsibility.

6.4 Access to official documents and information

As part of the decentralised Federal Administration, the OA-IA works on behalf of citizens. They have a right to know what the authorities are doing and how they are fulfilling their mandate. As a result, citizens have the right to gain access to information and at the same time the authorities have a duty to provide information.

The Freedom of Information Act (FoIA, SR 152.3) determines the scope and boundaries of passive information. Any person may request access to official documents without having to claim a special interest. The OA-IA did not receive any requests for access to official documents in the reporting year.

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 two hearings. The topics under discussion included the audit report for '22-13 Legended financial flows' (payments to undercover sources), the experiences of the OA-IA head during her first year in office, the development of the OA-IA's practice of issuing recommendations and the 2024 audit plan.

Federal Administrative Court (FAC)

As in previous years, the OA-IA met with representatives of the FAC. Topics for discussion included current FIS operations that had come before the FAC for authorisation of information gathering measures and current developments in cable communications intelligence.

Case law is continually evolving and the FAC is increasingly confronted with cyber-related technical issues. The OA-IA is also confronted with this challenge, as continuing digitalisation means that auditing activities are increasingly focused on information systems. The FAC and the OA-IA concluded that without information from the intelligence services on the technical context, it would be impossible for the FAC to make decisions on FIS requests for authorisation or for the OA-IA to carry out adequate audits.

Swiss Federal Audit Office (SFAO)

In addition to the abovementioned audit of the OA-IA, the following meetings were held with the SFAO:

- 20 February 2023: At this meeting, the Institute of Internal Auditors was presented to the OA-IA and the advantages and disadvantages of membership were discussed.

- 13 March 2023: Discussion of the protection criteria for employees who report harmful conduct in the Federal Administration (whistleblowing).

- 6 December 2023: The new mandate head for the DDPS introduced himself. Various aspects of coordination were discussed; if necessary, a coordination agreement should be developed in order to record the shared or diverging aspects of the various audit powers and thus avoid partial aspects of intelligence activities never being audited due to misunderstandings.

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

The OA-IA took part in all five ICA meetings.

The integration of its supervisory activities into the OA-IA, as planned by the revision of the IntelSA, has been delayed. For this reason, the OA-IA continues to support the work of the ICA within the framework of coordination and is currently refraining from further preparatory activities.

Federal Data Protection and Information Commissioner (FDPIC)

As part of its audit activities, the OA-IA reviews the information systems and data processing of the supervised authorities. It can also check the supervised bodies' retrieving of data that other, non-supervised federal authorities are responsible for processing. The FDPIC is the supervisory authority responsible for examining data processing by the federal authorities. The responsibilities of the FDPIC and the OA-IA – two authorities that are independent of the Federal Administration in the performance of their respective tasks – overlap to some extent. In order to avoid unclear responsibilities or duplication for the supervised authorities, the OA-IA and the FDPIC coordinate their activities at meetings and through regular exchange.

At a coordination meeting between the FDPIC and the head of the OA-IA in February 2023, it was agreed to formalise the current practice, which had been functional and expedient. In May 2023, the OA-IA and the FDPIC signed a coordination agreement.

Citizens

The OA-IA received 20 enquiries from citizens in 2023.

Other meetings

In 2023, the director of the OA-IA met at least once with the following people to discuss various matters:

- Head of DDPS
- Chief of the Armed Forces
- Head of DDPS General Secretariat
- Director and deputy director of FIS
- Head of MIS
- Head of EOC
- Head of DDPS Internal Audit
- Head of Operations Command
- Head of Cyber Command
- IS Advisor of DDPS
- ICA member

7.2 International contacts

The OA-IA can share oversight methods, processes and experiences with other oversight authorities working in the same field. This brings continuous benefits to audit activities. However, the OA-IA (unlike intelligence services) has no legal basis for substantive information sharing with foreign partner authorities. The following international meetings took place in 2023:

Online meeting with Canada's National Security and Intelligence Review Agency (NSIRA) on 27 April 2023

Following on from an NSIRA delegation visit to Bern on 17 November 2022, the two supervisory authorities held an online meeting on 27 April 2023.

At this meeting, the NSIRA presented its history, mandate and structure. The supervisory authority was created in 2019 and is an independent body that reports to Parliament. Its main tasks are to carry out inspections and process complaints. It reviews the legality, suitability, necessity and effectiveness of the national security and intelligence activities of all ministries and agencies of the Canadian government. It concludes reviews by issuing recommendations. The activities of the NSIRA are similar to those of the OA-IA. However, the NSIRA secretariat has more than 70 members of staff and its remit is much broader than that of the OA-IA. From an organisational point of view, given the evolution of

technology and its use in intelligence activities, the NSIRA benefits from the support of a specialised unit in this field.

Intelligence Oversight Working Group (IOWG)

The IOWG is an international working group comprised of representatives of the oversight authorities of Belgium, Denmark, the Netherlands, Norway, England, Sweden and Switzerland. Since November 2023, the Canadian authority NSIRA has had observer status in this working group for 2024.

IOWG staff level meeting, 25–26 May 2023, The Hague

The event began with participants presenting what had happened in their countries since the previous meeting in 2022. In future, the Netherlands will provide IOWG members with a digital platform to store presentations and administrative documents. Norway presented its communication methods and work procedures. Another topic concerned the use of cyber agents and member states' various legal regulations in this field. Particular attention should be paid here to the distinction from OSINT. Finally, a technical expert from the Dutch supervisory authority presented his thoughts on AI and automated decision-making. There was a consensus that the services and their supervisory bodies need to address this topic in more detail.

IOWG staff level meeting, 8 November 2023, Oslo

On 8 November 2023 the staff level of the IOWG met for a preparatory meeting for the chair level meeting the following day. Work focused largely on drafting an agenda proposal for the next year's meetings. The following topics were proposed:

- Commercially acquired datasets used by supervised services.
- Organisation of an online exchange on certain topics between the IOWG meetings.
- Exchange on the rules and practices of personnel security screening in the different IOWG countries.
- Discussion of possible international forms of cooperation between the supervisory bodies.
- Presentation of general oversight methods in the different countries.

IOWG chair level meeting, 9 November 2023, Oslo

The heads of the various supervisory bodies met on 9 November 2023. The proposed agenda at staff level was approved and all sides especially welcomes an in-depth discussion of methodology. At their request, the Canadian supervisory authority will be granted observer status within the IOWG.

IOWG meeting with a US authority and various non-governmental organisations (NGOs) on 27 November 2023, Washington DC

The IOWG organised a meeting with the Privacy and Civil Liberties Oversight Board (PCLOB) on the margins of the International Intelligence Oversight Forum (IIOF) (see below). The PCLOB is an independent agency within the executive branch established by the 9/11 Commission Act of 2007. The bipartisan, five-member board is appointed by the President and confirmed by the Senate. The Chairman is a full-time member of staff, while the four other members of the committee serve in a part-time capacity. The committee's task is to ensure that the federal government's efforts to prevent terrorism are reconciled with the need to protect privacy and civil liberties. Of particular interest was the exchange on the term 'open' in open-source intelligence (OSINT) and the rapid development and use of AI resources.

In the afternoon, meetings took place at the Center for Democracy & Technology and other NGOs. OSINT-related information gathering, in particular the use of data brokers, was also widely discussed here. The exchange then focused on the question of whether or how the intelligence services could

share information and thereby circumvent the authorisation requirement for such information gathering.

European Intelligence Oversight Conference (EIOC), 9–10 November 2023, Oslo

This year's varied conference programme included topics such as:

- Oversight methods in general;
- intelligence services' disproportionate use of publicly available data and measures to be taken;
- fundamental exchange on the recent case law of the European Court of Human Rights;
- technical oversight methods;
- aspects of communication by supervisory authorities.

The event offered the OA-IA a good opportunity for in-person dialogue with fellow conference participants on oversight methods and legal conditions.

International Intelligence Oversight Forum (IIOF), 28–29 November 2023, Washington DC

The sixth IIOF meeting took place at the American University Washington College of Law on 28 and 29 November 2023. In addition to the OA-IA head and a member of staff, forum participants included members of administrative and parliamentary intelligence oversight authorities and representatives of intelligence services, data protection authorities and NGOs.

Discussion topics included:

- Necessary and appropriate oversight: protecting private life and national security on both sides of the Atlantic;
- the significance and consequences of the 14 December 2022 OECD Declaration on Government Access to Personal Data Held by Private Sector Entities;
- good practices on integrating guarantees into intelligence services' operations;
- similar challenges, different framework conditions: comparing how countries regulate the activities of their intelligence services.
- Article 11 of the Council of Europe's Convention 108+: current status, challenges and findings.

After numerous presentations and discussions, forum participants visited the Intelligence Community Campus in Bethesda. The visit included a discussion of the resources employed by the US intelligence service to ensure the consistent balance between national security interests and respect for citizens' fundamental rights in accordance with the law.

The forum's thematic scope and the opportunities it provides to interact with other services and authorities are enormously valuable for the OA-IA. It also allows the oversight authorities to learn from the critical and often constructive perspective of the research community (universities, NGOs, etc.). The diversity of approaches to supervisory activities – stemming from the different legal and cultural framework conditions – as well as the limitations and challenges associated with supervisory work enable the OA-IA to analyse, develop and improve its practice.

8 Appendix

8.1 Audit Plan for 2023

No	Title	Entity to be audited
Strategy and Planning		
23-1	Generation and impact of Federal Intelligence Service (FIS) products	FIS
Organisation		
23-2	Legal services	FIS
23-3	Protection and security	FIS
23-4	IT Business Continuity Management and Disaster Recovery	FIS
Cooperation		
23-5	Lucerne Cantonal Intelligence Service (CIS)	CIS / FIS
23-6	Nidwalden CIS	CIS / FIS
23-7	Obwalden CIS	CIS / FIS
23-8	Uri CIS	CIS / FIS
23-9	Management of technical sensor's mandates at the Electronic Operations Centre (EOC)	EOC
23-10	Cooperation between the FIS and private individuals and/or entities	FIS
Information gathering		
23-11	Operations, operational investigation and intelligence-gathering activities requiring authorization	FIS
23-12	Human intelligence (HUMINT)	FIS
23-13	Use of virtual agents	FIS
Resources		
23-14	Implementation of OA-IA recommendations	FIS / MIS[4] / EOC
Data processing and archiving		
23-15	Compliance with the right to receive information	FIS
23-16	Information systems, data storage systems and data files outside the scope of Article 47 Intelligence Service Act	FIS

[4] Military Intelligence Service

8.2 Abbreviations

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
EOC	Electronic Operations Centre
FAC	Federal Administrative Court
FADP	Federal Act of 25 September 2020 on Data Protection (Data Protection Act, SR 235.1)
FDPIC	Federal Data Protection and Information Commissioner
FIS	Federal Intelligence Service
ff.	and following
HUMINT	Use of human sources
ICA	Independent Control Authority for Radio and Cable Communications Intelligence
ICT	information and communications technology
IIOF	International Intelligence Oversight Forum
IntelSA	Federal Act of 25 September 2015 on the Intelligence Service (Intelligence Service Act; SR 121)
IOWG	Intelligence Oversight Working Group
ISACA	Information Systems Audit and Control Association
MIS	Military Intelligence Service
NGO	non-governmental organisation
NSIRA	National Security and Intelligence Review Agency
OA-IA	Independent Oversight Authority for Intelligence Activities
OAI	online alias identity
OP	operations
OSINF	open-source information
OSINT	open-source intelligence, gathering information from public sources
para.	paragraph
PDCS	providers of derived communications services
PCLOB	Privacy and Civil Liberties Oversight Board
PTSS	Post and Telecommunications Surveillance Service
ITSCM	Information Technology Service Continuity Management
SFA	Swiss Federal Archives
SFAO	Swiss Federal Audit Office
SPTA	Federal Act of 18 March 2016 on the Surveillance of Post and Telecommunications (SR 780.1)
SR	Classified Compilation of Federal Legislation