Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

**Independent Oversight Authority for Intelligence Activities**

# Annual Report 2018
## of the Independent Oversight Authority for Intelligence Activities OA-IA

### → The Intelligence Service Act

The Intelligence Service Act (ISA) came into force on 1 September 2017 – together with three related ordinances: one on the intelligence service (ISO), one on the FIS information and storage systems (ISSO-FIS) and one on the supervision of intelligence activities (OSIA). The ISA replaced the Federal Act on Responsibilities in the Area of the Civilian Intelligence Service (CivISA) and the Federal Act on Measures to Safeguard Internal Security (MSIS). The ISA regulates all intelligence activities comprehensively and formulates the mandate for a full situation assessment by the Federal Intelligence Service (FIS) for the benefit of its clients. The ISA is intended to increase security in Switzerland and to assist in safeguarding vital national interests. The Federal Council may therefore take action in accordance with the FIS to protect basic constitutional order, foreign policy and Switzerland as a centre for employment, business and finance.



# 1. Summary
## Oversight and transparency

The disclosures made by the whistle-blower Edward Snowden in 2013 brought it to everyone's attention that intelligence services intercept and evaluate a wide range of electronic data and signals that are circulating around the world.

These breaches of individuals' privacy caused widespread concerns and also became an important issue in the debate on the new Intelligence Service Act (ISA) in Parliament.. The Independent Oversight Authority for Intelligence Activities OA-IA takes its duty of oversight seriously, based on principle 'We strengthen trust'. It reviews the legality, expediency and effectiveness of intelligence service activities, thereby providing the public with a degree of more transparency with regard to these activities. The Authority intends to continue with this task in the coming years, while guaranteeing its independence.

On 25 September 2016, almost two-thirds of voters agreed to accept the new ISA and the independent oversight of intelligence activities that it brings. The clear support in Parliament and in the referendum came about not least because Parliament wanted to bolster the oversight of the intelligence service by introducing an independent oversight authority. In return, the intelligence service was given new, far-reaching surveillance powers. They not only included the power to bug rooms, but also the power to read e-mails or eavesdrop on telephone conversations.

In May 2017, the Federal Council appointed Thomas Fritschi to the post of Director of the OA-IA for a term of six years. The OA-IA exercises its function independently and free from any directives. It has its own budget and employs its own staff. The OA-IA is based in Bern.

The process of establishing the Authority, which began at the end of 2017, continued in 2018. The OA-IA set itself up in the report year, conducted thirteen audits of intelligence services in parallel and also recruited its staff. In addition, it passed on its advice and recommendations to the Head of the DDPS, who in turn instructed the intelligence services concerned to implement, in full and without modification, all the recommendations made in the reports that he had considered by the end of year. The new Act provides the OA-IA with three core tasks: Its most important activity is the supervision of the intelligence activities of the Federal Intelligence Service (FIS), of the Armed Forces Intelligence Service (AFIS), the cantonal executive authorities, and of third parties and other agencies to which duties have been delegated. It also coordinates its activities with other federal and cantonal oversight bodies. Lastly, it provides the public with information on its activities in an annual report.

The OA-IA concluded in 2018 that the FIS is able to use its new powers and indeed is doing so. Having a broader palette of information gathering measures leads to additional expenditure. As more experience is gained, it will be possible to further optimise procedures. New and complex requirements apply to intelligence activities in the Armed Forces – based on the new Act and especially in technical areas. These challenges are being met effectively, although there is still potential for improvement in the regulatory environment.

# 2. Table of Contents

**1. Summary** 3
Oversight and transparency 3

**2. Table of Contents** 4

**3. Personal** 5
We strengthen trust 5

**4. Development of the independent oversight authority** 6
4.1 History and legal background 6
4.2 Embedded in the regulatory landscape 7
4.3 Priorities under development 8
4.4 The staff 8
4.5 The organisational challenges 9

**5. Supervisory activities** 10
5.1 Audit process 12
5.2 Audits at the FIS 13
5.3 Audits at the AFIS and the EOC 16
5.4 Supervision in the cantons 18
5.5 Acceptance 18

**6. Coordination** 21
6.1 Contacts with other bodies and agencies 21
6.2 Contact with international agencies 23

**7. A view from outside (carte blanche)** 25

**8. Key figures as of 31.12.2018** 28

**9. Annex** 29
9.1 2018 Audit Plan 29
9.2 List of abbreviations 30



# 3. Personal
## We strengthen trust

Thomas Fritschi, Director of the OA-IA

"I remind you again: by a clear majority, voters on 25 September 2016 approved Switzerland's new Intelligence Service Act (ISA), the first act in this form. Several serious terrorist attacks had rocked Europe in the months before the vote. At the same time, the Snowden Affair highlighted the problems associated with intelligence activities. The need for stronger defences and preventive measures to protect our society, our values and our freedoms seemed obvious."

"The new Act created an independent oversight body."

With the new Act, which gave the Federal Intelligence Service (FIS) considerably more powers, an independent oversight body was also created. This supervises the intelligence activities of the FIS, the cantonal executive authorities and the third parties and other agencies delegated tasks by the FIS. With the new Act, the FIS has been given a clearly more effective arsenal of intelligence resources that are by their very nature also capable of compromising the freedoms of people living in Switzerland. The Act therefore lays down a strict framework for using these resources. The OA-IA interacts with other supervisory bodies in fulfilling its duty to monitor compliance with these limits. Through our work, we aim to, for example

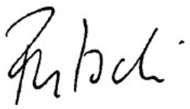
- check compliance with deletion deadlines for data files
- scrutinise the ordering and conduct of intelligence operations
- assess the preparations made by the services in view of the potential risks that may arise
- ask questions about national and international cooperation between services

and thus strengthen trust in intelligence activities as a whole.

Finding the right staff for the OA-IA, i.e. employees with the required expertise who could at the same time preserve their independence, was a demanding task. All posts could be filled within a reasonable period of time. We carry out our tasks wherever we are required to go and in consultation with intelligence service staff.

We see the challenges for the intelligence services – and thus also for supervision – of resource management for intelligence activities; in the growing demands placed on those conducting counter-espionage; these challenges include hacker attacks on the data of state institutions, of private individuals, and of large and small businesses as well as the constant progress with digitalisation.

In 2018 we carried out thirteen audits and made our first national and international contacts. We plan to continue with and expand this in 2019 – in order to pursue, develop and enhance our vision: We strengthen trust.



**Thomas Fritschi, Director of the OA-IA**

PS: You will find our audit plan for 2019 here:
www.ad-nd.admin.ch

# 4. Development of the independent oversight authority

## 4.1 History and legal background

While intelligence activities have a long history, that of the oversight of the intelligence activities is rather shorter. Oversight often has its basis in scandals and criminal mismanagement and results from coming to terms with such incidents. For example, the Control Delegation (CDel) was set up as a parliamentary oversight body in response to the so-called Secret Files Scandal at the start of the 1990s, and was also involved in 2016 in the inquiry into the activities of Daniel M.

The OA-IA is not the direct product of a domestic scandal, but rather of the political debates surrounding the new Intelligence Service Act, which came into force on 1 September 2017. The OA-IA acts on the basis of Article 76 of the Intelligence Service Act.

An intelligence service oversight body had already been created with the merger of the Strategic Intelligence Service and the Service for Analysis and Prevention in 2010. This body was part of the General Secretariat of the DDPS and as a consequence did not have the independence enjoyed by today's supervisory authority. With the additional powers that the FIS acquired under the new Act, the need for supervision became greater. The intelligence services are now permitted to use new procedures such as cable communications intelligence, tracking of persons or searching buildings and premises. These new options lead to reduced privacy for the persons under surveillance. In the original draft of the Act, a continuation of the existing system of supervision was planned. As a consequence of reports in the media linked to the Snowden Affair, public concerns began to grow about the intelligence services' new surveillance powers. The political debate in Parliament led to the creation of an independent supervisory body for the intelligence activities of the FIS, the cantonal executive authorities and of third parties and other agencies that are delegated tasks by the FIS under the ISA. The supervisory power over the Armed Forces Intelligence Service is based on Article 12 of the Ordinance on the Armed Forces Intelligence Service [1]. The connection between the DDPS and the new supervisory body is now purely administrative.

[1] O-AFIS: SR 510.291

### → Edward Snowden

Edward Joseph "Ed" Snowden is an American whistleblower and former CIA employee. His revelations provided insights into the extent of the worldwide surveillance and espionage practices of intelligence services - predominantly in the United States and Great Britain. They triggered the NSA affair in the summer of 2013.

### → Daniel Moser

On 28 April 2017 Daniel Moser (Daniel M.), a former source for the Federal Intelligence Service (FIS), was arrested in Frankfurt am Main on suspicion of espionage. The case caused a sensation in Switzerland. On 24 May 2017, the Control Delegation (CDel) decided to investigate the background to the case and the role of the FIS, the Federal Council and the Office of the Attorney General of Switzerland. Daniel Moser managed foreign intelligence gathering for the FIS as a recruited source from July 2010 until the end of May 2014.



"The challenge we face is reflected in the increased demands placed on and opportunities available for intelligence activities."

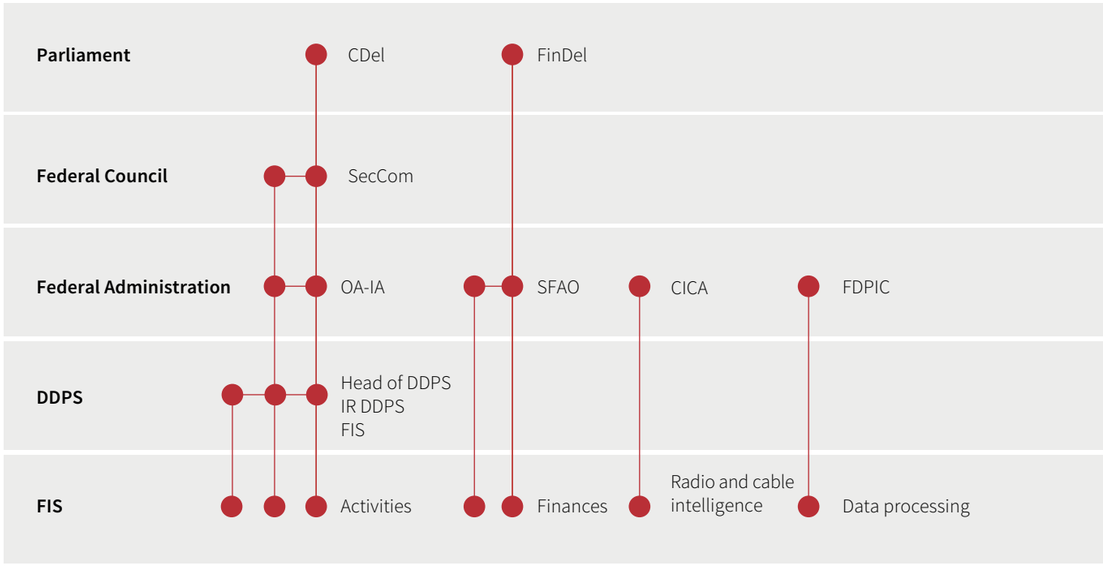
## 4.2 Embedded in the regulatory landscape

In addition to the OA-IA, other authorities are responsible for supervising intelligence activities. The OA-IA has a duty to coordinate with these other supervisory bodies. It is the only supervisory authority at Federal Administration level that deals exclusively with all intelligence activities. Parliamentary oversight is the responsibility of the Control Delegation (CDel).

### → The core tasks of the Federal Intelligence Service

The core tasks of the Federal Intelligence Service FIS are prevention and situation assessment. It does this primarily for the Federal Council, the cantonal security agencies, the federal departments and military command. All FIS activities are subject to a process of continuous checks – in particular by the DDPS, the Federal Council, the Control Delegation of Parliament (CDel) and the Independent Oversight Authority for Intelligence Activities (OA-IA).

Supervisory bodies responsible for the FIS



“The disclosure of our audit plan is an important part of our transparent approach.”

## 4.3 Priorities under development

Supervising and assessing the legality, expediency and effectiveness of intelligence activities requires a variety of abilities. First of all, detailed knowledge of intelligence work is needed. In addition, knowledge of the auditing process and other expertise is required, for example in data protection law, new technologies, information technology and political developments. Staff impartiality is a further important criterion. And furthermore: the official Swiss languages and a gender balance must be taken into account.

The size and structure of the authority have also been defined. An analysis was made of what the new authority required and empirical values from the former intelligence oversight system and models of comparable of foreign supervisory bodies were considered.

The additional powers of the FIS, the audit environment at federal level and in the cantons and the structure of authorities in comparable countries (for example Belgium) led to a request for the appointment of a team of ten full-time staff. This has been budgeted for and approved by Parliament as part of the Confederation’s Integrated Plans for Tasks and Finances (IAFP). The new authority has a flat hierarchy, the management chains are short.

The new legislation provides for the authority to be based in Bern. This makes sense, given that the FIS headquarters are nearby. The work that the OA-IA does requires that its offices are secure. The fact that the OA-IA is assigned for administrative purposes to the GS-DDPS comes as a result of the geographical proximity of the two authorities, while the OA-IA’s independence confirms its distance from the GS-DDPS. After around a year in separate offices in the same building as the GS-DDPS, the OA-IA moved in autumn 2018 to its own premises. The new building meets all the requirements in full.

Parliament approved a budget for the OA-IA for 2018 of 2.3 million francs. This includes 1.8 million francs for all staff costs. This corresponds to ten full-time positions.

## 4.4 The staff

Recruitment was carried out in two phases. Immediately after the Director began work, four employees were recruited. Following approval of the budgets, a further five employees were sought, assessed and appointed in a second phase at the beginning of 2018. A programme was created for their induction. This includes attending the training modules for new FIS employees, an introductory visit to the Military Intelligence Service (MIS) and to the Electronic Operations Centre (EOC). In addition, the new employees were given introductions to the theoretical, administrative and organisational aspects of their new jobs.

All vacancies at the OA-IA have been filled since 1 September 2018. The staff comprises four women and six men. Three employees are French speakers, one bilingual in French/Italian and seven employees are German speakers. The employees come with expertise and experience in intelligence activities, police work, prosecution, auditing, accounting, data protection, law, criminology and information technology. It is also important that the employees are up-to-date with technical, professional and legal developments. In addition, they have to be ready to question the existing situation critically. The OA-IA therefore creates a climate of open internal communication.



## 4.5 The organisational challenges

The OA-IA is independent and part of the DDPS for purely administrative purposes. It is therefore one of a group of independent supervisory bodies (such as Supervisory Authority for the Office of the Attorney General [SA-OAG] or the National Commission for the Prevention of Torture [NCPT]). Basically, all these supervisory bodies differ to some extent in their structure. Their similarity lies in their need to define certain structures and procedures. Under Article 3 OSIA, the OA-IA must draw up and publish its own procedural rules. On 26 February 2018, following a brief consultation process, these rules were adopted and published in the Official Federal Gazette. Since the start of May 2018, the OA-IA has also had its own website (www.ab-nd.admin.ch), on which the procedural rules are also publicly accessible.

In addition to the procedural rules and the website, other principles have been and are being adopted. The aim is to ensure that the OA-IA can comply with and fulfil the requirements of the legal framework that has been set out for it. Essential aspects of this, for example, are rules on who can act and sign for the authority and a risk management system. In addition, organisational and audit manuals are being drawn up to describe the most important procedures and requirements. These projects began in the report year and different degrees of progress have been made, although the aim is to complete all the work in 2019.

### → Code of Conduct

The staff of the OA-IA are subject to federal procedural guidelines defined and issued by the Federal Office of Personnel. In order to safeguard the independence of the OA-IA, it is important that all employees define and apply these values in a uniform manner. The OA-IA has held a wide-ranging discussion on the content of the guidelines and where necessary, defined its own code of conduct.

# 5. Supervisory activities

Ground-breaking work was required before the OA-IA could be established – a review and outlook.

Every year, the OA-IA draws up a risk-oriented audit plan. This also serves the OA-IA as a planning instrument. Following a first audit in 2017, which related to the readiness of the FIS for the introduction of the new Act, in 2018 it was planned to conduct audits on a more risk-oriented basis and in all areas of intelligence activities. The other supervisory bodies in the intelligence sector (see the diagram above) were sent the audit plan at the end of December 2017 for their information. In addition, the OA-IA published the audit plan at the start of May 2018 on its website. A total of twelve audits were planned for 2018. At the same time, two further partial audits were included by splitting audits 18-1 and 18-9 in the plan. The subjects of the audits were: the FIS (eight audits), the Armed Forces Intelligence Service (two audits) and the Electronic Operations Centre (three audits). In addition, the OA-IA conducted a survey of the cantons and organised a conference with the cantonal oversight bodies.
Seven of the audits in the 2018 plan were exploratory in nature. They aimed to weigh up relevant information on the basis of risk as the starting point for further OA-IA inspections. In addition, the OA-IA is running an audit theme memorandum, to store potential subjects for audit that arise in the course of the year.
In September 2018, the focus was on drawing up the risk-oriented audit plan for 2019. Based on the audit theme memorandum, the OA-IA identified seven areas where an audit may be required. The future audit plans for the OA-IA should include audits in each of these areas:

- **Strategy and planning:** In this area, an examination should be made of how intelligence organisations in Switzerland set their short, medium and long-term objectives and how they intend to achieve these objectives.

- **Organisation:** The intelligence services rely on being suitably structured and having appropriate procedures in order to make their activities as effective as possible.

- **Cooperation:** Cooperation with the intelligence services' national and international partners and stakeholders is based on clear legal principles, yet is exposed to certain risks.

- **Information gathering measures requiring approval:** Information gathering measures requiring approval encroach profoundly on the private domain of the persons concerned. The Federal Administrative Court examines and authorises the measures and, if necessary, imposes conditions and requirements that the intelligence services must comply with. The OA-IA checks compliance with these judicially imposed conditions and the processing in the systems of the information gathered using these measures.

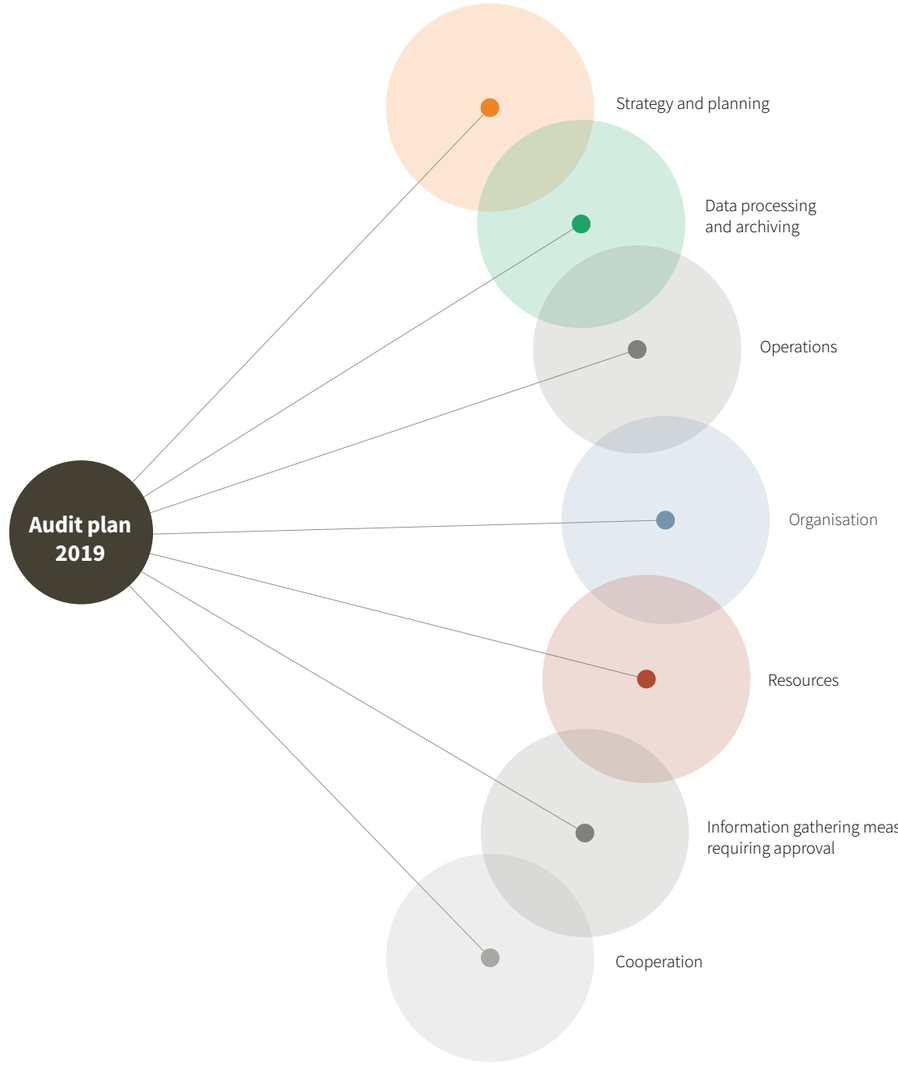
- **Operations:** Conducting operations to gather information is part of the main business of the intelligence services. The IntelSO[2] regulates both the start and conclusion of operations and reporting on the results. Conducting these operations carries risks; accordingly, the OA-IA reviews the operations with regard to their legality, expediency and effectiveness.

- **Resources:** The OA-IA checks that resources are used appropriately and effectively as this is essential for conducting intelligence service activities efficiently.

- **Data processing and archiving:** Gathering and processing information is the core business of the intelligence services. In view of the sensitivity and the need to protect the processed data, this is subject to comprehensive and complex legal requirements; the OA-IA verifies compliance with these requirements.

[2] SR 121.1





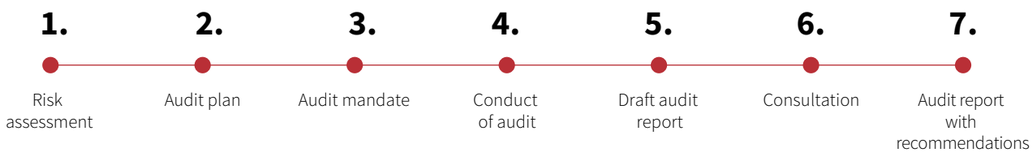

Each year, the OA-IA will analyse the potential audits stored in the audit theme memorandum and weigh up their importance based on the risks involved. The audit plan for the following year is drawn up on the basis of this analysis and sent to the other auditing bodies before the start of the new audit report period.

The OA-IA can also carry out unannounced audits, in addition to the audits that are planned and subject to advance notice. The OA-IA has also carried out written inquiries, in some cases based on reports in the media – for example, the inquiry relating to the fake psychologist [3].

[3] Tagesanzeiger 09.06.2018

“The prudent development of the annual audit plan is elementary.»

## 5.1 Audit process




**Plan**

The OA-IA draws up an annual audit plan based on the risks with audit numbers and titles

**Action**

The audit managers conduct audit activities at the agencies concerned (interviews, inspections, etc.)

**Consultation**

The agency concerned can comment on the draft report



## 5.2 Audits at the FIS

**18-1 Overview of the FIS data landscape and content of the residual data memory**

The FIS has designed its information systems to comply with the new ISA. The OA-IA used this audit to obtain an overview of the data landscape that will serve as the basis for future audits of the information systems. One part of the audit involved making a comprehensive compilation of the legal requirements and the internal organisational documentation. A second part involved reviewing the residual data memory system to verify its compliance with the law.

The residual data memory stores data that, when obtained, cannot be immediately assigned to any of the other FIS systems. This can lead to data being retained for a disproportionate length of time. In 2018, the FIS’s own compliance and quality assurance sections also reviewed the residual data memory. Both sections concluded that the data processing is carried out lawfully.

The OA-IA found that only specifc data were stored in the residual data memory as preliminary storage location for another information system. The data contained in it at the time of testing were processed legally.

The OA-IA ultimately recommended the adaptation of certain entries in information systems in the register of the Federal Data Protection and Information Commissioner (FDPIC).

**Audit 18- 1a Functionalities of statistics programmes in databases**

In Audit 18-1a, the OA-IA tested whether the statistics programmes in the information and storage systems of the FIS worked correctly. In particular, it examined whether the figures supplied allow a reliable check to be carried out on the development of the data collections and an appropriate comparison between the systems.

The FIS uses its statistics programmes both in its management of internal activities and when passing data on to external agencies.

The OA-IA found that the FIS is using a sufficient number of statistics programmes and knows how to use these programs appropriately. Efficiency could be increased through the integration of the information systems and the resulting higher combinability of the retrieval methods.

**18-2 Electronic work aids in the workplace**

The most important objective was the review of the legality of the use and storage of individual working data by FIS members of staff.

A main task of the FIS is to gather and process information with the aim of identifying threats to internal and external security at an early stage and initiating the required measures. The statutory requirements regulate the information flows and in particular the feeding of the information concerned into the Service’s information systems. The FIS defines individual working data as data that have a connection with its working processes and that are used exclusively by the individual member of staff concerned. The legislation that the FIS must comply with includes the Federal Data Protection Act [4], which regulates the processing of personal data. Data that is processed exclusively for personal use are excluded from the

[4] SR 235.1

“To ensure an objective result, we always check in pairs.”

scope of application of the Data Protection Act. This provision must be construed restrictively and may not be used to justify the secret processing and storage of data.

The OA-IA noted while conducting the audit that individual working data were being used at all ten work stations used by the members of staff. The FIS regulates the processing of this data in various concepts, directives and regulations. As the term “individual working data” is not used in an entirely uniform manner, this leads to the members of staff making different interpretations of the term. The OA-IA therefore recommended that further explanatory information be added to the regulations. In addition, there was a lack of awareness of some of the forms of data storage, as they are not mentioned in the relevant legal provisions. The OA-IA therefore recommended that the ISSO-FIS be amended accordingly when it is next revised. Likewise, the FIS should raise the awareness of its members of staff that they should in principle delete individual working data that is no longer required. In addition, it should provide them with better information on surveillance measures used to check on instances of access to the information systems.

In addition to this primary objective, an audit procedure that complies with data protection law should be developed beforehand, so that members of staff at the work stations can obtain an overview without having to give notice a long time in advance.

**18-3 Compliance with requirements when implementing IGMRA**

In Audit 18-3, the OA-IA examined compliance with the requirements when implementing information-gathering measures requiring approval (IGMRA). The OA-IA checked whether the FIS complied with the requirements and restrictions in the approved IGMRA. Following an initial meeting with the FIS in which the requirements were discussed, the auditor managers reviewed all the approval decisions made by the Federal Administrative Court. They also checked all the approvals issued by the Head of the DDPS between the ISA coming into force on 1 September 2017 and the start of the audit. They compared these with the information provided by the FIS. Further audit issues demanded structured interviews and on-site visits. Here the OA-IA found that the FIS generally dealt with the requirements diligently and respected the restrictions imposed on the implementation of IGMRAs. In one case, the FIS however failed to comply with a restriction imposed by the Federal Administrative Court: it did not inform the court of the results of the IGMRA within the given deadline.

The FIS complies with the required limits in relation to software used to intrude into computer systems and networks. The automation of operational tasks using email reminders is currently being developed.

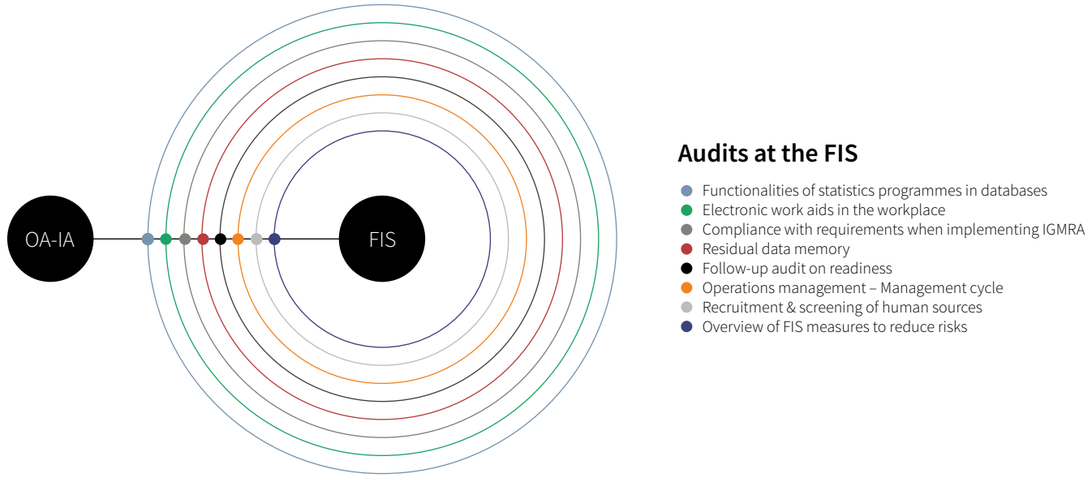
As a result of the FIS’s proactive attitude, the OA-IA has decided at this stage not to recommend any further automation measures. It will leave it for the time being to the FIS to develop the required tools. Lastly, the OA-IA has proposed describing an internal process that applies specially in relation to requirements in the IGMRA procedures. In addition, the agency responsible for conducting operations should ensure that all relevant information is included in its file and that its files are given a classification that means they may easily be consulted.

**18-4 Follow-up audit on readiness**

Audit 18-4 was a follow-up on the first audit the OA-IA carried out, in in 2017. Essentially, in this audit the OA-IA noted that the FIS interfaces with the prosecution authorities had to be regulated in more detail and in consultation with the relevant partners. Recommendation 9 in the Control Delegation report on the case of Daniel M. [5] also raised this issue. In 2018, therefore, the OA-IA decided not to carry out this follow-up audit. The recommendations are being reviewed as part of the controlling process.

[5] Inspection as a consequence of the arrest of a former FIS source in Germany, Report from the Federal Assembly Control Delegation dated 13 March 2018, BBL 2018 5045.






**18-5 Operations management – Management cycle**

In Audit 18-5, the OA-IA took a closer look at operations management and the management cycle. The focus was the conduct of operations within the FIS, in order that the OA-IA could evaluate the risks and the measures taken in connection with information gathering. The resultant residual risks serve as the basis for subsequent audits of operations.

For the purposes of this audit, the process of conducting FIS operations was divided into partial processes, i.e.

- activities before the start of an operation
- defining the resources required for an operation
- cooperation with partners on an operation
- the form in which the operation is started
- conducting the operation
- reporting, assessment, efficiency and costs of an operation
- concluding the operation

The questions asked and the documents consulted were intended to make it possible to understand the problems, context and the chosen procedure for each stage of the operations.

A year after the ISA came into force, the FIS was conducting its operations satisfactorily. An operation is clearly defined in accordance with Article 12 of the Intelligence Service Ordinance, begun, formally concluded and separately documented. The efficiency with which operations are conducted can be improved by systematically structuring the procedure from start to finish. The results of the operation are entered in the IASA information system after a certain delay.

**18-6 Recruitment & screening of human sources**

In Audit 18-6, the OA-IA considered human sources. It looked at the question of how the FIS recruits and screens these sources. The OA-IA noted that there is a set process for the recruitment, management and discharge of human sources and that the individual procedural steps are comprehensively documented. The FIS has adjusted its rules on this. There are control measures and requirements for the documentation on source management. It is now important to implement these rules. The FIS internal documentation on persons offering unsolicited information must be standardised and harmonised in order to obtain a better overview and make it more comprehensible.

**18-10 Overview of FIS measures to reduce risks (incl. check of the cantonal intelligence services (CIS) by the FIS)**

In Audit 18-10 the OA-IA noted that the FIS measures to reduce risks, i.e. risk management, compliance, the management system for information security, controlling, security and quality assurance are in place, appropriately developed and effective. The objective was to obtain an overview of how risks related to FIS activities are identified, assessed, managed and minimised. An assessment was made of whether these areas are adequately covered by measures to reduce risks and therefore effective. The OA-IA was also able to draw up its audit plan for 2019 on the basis of the recognised remaining residual risks that the FIS has to contend with.

All the other risk-reducing management systems are connected to the FIS risk management system. These include, for example, the incident management system, the management system for information security; the quality assurance system, which carries out summary checks and random tests in relation to the legality of data processing in the FIS information systems and makes recommendations or a current data protection concept, which covers the tasks in all areas and under which the data collections have to be registered with the FDPIC.

The OA-IA found that the decentralisation of quality assurance under the ISA has reduced its effectiveness and no assessment has been made of the cost-effectiveness of individual organisational units.

The audit recommendations related to the data protection consulting tasks in the data protection concept, which have to be applied in all fields of FIS activity (which the OA-IA was able to verify before finalising the audit report), the drafting of a concept for implementing checks in the CIS, and completing the impact dimension assessment and the revision of the damage descriptions for each impact dimension.

## 5.3 Audits at the AFIS and the EOC

**Audit 18-7: Composition of the organisation and assignments carried out by the intelligence units in the Armed Forces**

In Audit 18-7, the OA-IA determined the principles required to gain an overview of how the intelligence units in the Armed Forces are organised and carry out their tasks.

The audit activities included structured interviews and an inspection of documents. The statements in the inspection report primarily summarised what the MIS staff themselves said and the findings made from examining the documents received. The statements made were not verified in detail. As result of the audit, an overview of Armed Forces units active in the field of intelligence is now available.

In addition, the audit revealed that some tasks, directives and regulations have still to be adapted to the new structures under the Swiss Armed Forces Development Programme (AFD) and to the new statutory regime. Up-to-date tasks, directives and regulations are a basic requirement for guaranteeing legal certainty and reliability. Moreover, it was found that although the term “Armed Forces Intelligence Service” was clearly defined, the overall responsibility for the organisation of the AFIS was not clearly assigned to any organisational unit, in particular the MIS. The OA-IA made recommendations on both these findings.

**Audit 18-9 Review of the selectors in the system**

The subject of Audit 18-9 was the management of selectors by the Electronic Operations Centre (EOC). The aim was to examine the generation, control and possible adaptations of selectors for gathering information. In general, it was established that the EOC is managing selectors effectively.

Three random tests failed to reveal any indication of unlawful selectors. However, 20 per cent of the selectors commissioned by the FIS were not recorded in the EOC systems. The EOC’s dynamic practice for gathering information is adequate. From a legal point of view, it seems doubtful that the EOC’s method of information gathering complies with Article 2 paragraph 5 of the Ordinance on Electronic Warfare and Radio Communications Intelligence [6] and thus it probably does not have a sufficiently precise legal basis. This provision can be interpreted in different ways and is thus unclear. The OA-IA therefore recommended that the head of the DDPS should amend the Ordinance to reflect the method of information gathering used by the EOC. Article 2 paragraph 5 EWRIO, on which it is based, does not however provide an adequate basis. The OA-IA therefore recommends that the EWRIO be made more precise on this point.

**Audit 18-9a overview of the EOC data landscape**

This subject o the audit was removed from audit 18-9 and postponed to 2019 as a separate audit.

**Audit 18-11 Overview of measures to reduce risks in the MIS**

In Audit 18-11, the OA-IA analysed the extent to which the Military Intelligence Service took measures in the areas of risk management, security, quality assurance, compliance, data protection and controlling in order to minimise its risks as much as possible.

The OA-IA held interviews with various representatives of the service and with the persons responsible at the DDPS and examined documents. The MIS is integrated into the complex structure of the Department. In comparison with the size of the Department, it is a small organisation and dependent on services provided by the DDPS. It is bound by legal requirements set at departmental level. In order to comply with these requirements, the MIS incurs administrative costs. For example, an overall risk management system is under development in the Defence Group, but the MIS will only be included in this at a later date. The specialists for compliance and data protection are also found at defence level, which makes it difficult to provide specific support services to the MIS.

In relation to IT interfaces, in the near future the MIS will require support from the Armed Forces Staff (ASTAB) and the Armed Forces Command Support Organisation (AFCSO). The MIS is surrounded by systems that are so diverse and complex that they make the efficient and effective processing of information very difficult.

“Our recommendations must generate added value.”

**Audit 18-12 Overview of measures to reduce risks at the EOC**

18-12 was the last of three audits (18-10, 18-11 and 18-12) that reviewed the measures that the organisation itself takes to reduce risks.
The interviews and the analysed documentation revealed that the EOC takes measures to reduce risks in certain areas, particularly in relation to security. In the other areas, there is a need to catch up that is also causing the EOC to incur a certain amount of administrative expenditure. In view of the sensitivity of the information processed and the EOC’s important security tasks, the OA-IA issued some recommendations with the aim that the organisation improve the analysis and control of its own risks.

[6] VEKF, SR 510.292



### → Selectors

Selectors are all types of strings (for example telephone numbers) that are used in the EOC systems. They enable the control of information recorded by the EOC that has to be stored as a priority (primary selectors) and also facilitate searches for relevant content in the stored data (secondary selectors).

## 5.4 Supervision in the cantons

With the entry into force of the ISA on 1 September 2017, the supervision of the cantonal intelligence services became expressly regulated in a federal act. In addition, minimum requirements for the cantonal supervisory bodies (CSBs) were introduced at ordinance level.

In 2018, the OA-IA conducted a survey of the current supervisory organisational structures and practices as well as the needs of the CSBs for the cantonal intelligence services (CIS). All the CSBs participated in the survey and submitted their responses. All the cantons have implemented the legal requirements adequately.

The OA-IA informed the CSBs of the results of the survey at the first OA-IA -conference in August 2018. On 23 August 2018, 48 representatives from 23 cantons and the Confederation met in Bern for their first discussion about the supervision of intelligence activities. The aim was for them to inform each other about how they were carrying out their supervisory duties and to exchange reports on experiences from the individual cantons and on selected topics.

The FIS carries out intelligence service activities with and in the cantons. It is the duty of the cantons to conduct suitable checks on the cantonal executive agencies. All the cantons comply with this duty using a variety of models. The models used by the cantons of Fribourg and Basel-Stadt were presented at the conference and the issues of data protection and auditing were discussed.

The OA-IA coordinates with the cantonal supervisory authorities and sends any recommendation not only to the Head of the DDPS but also to the cantonal supervisory body concerned. A valuable basis has been established for future audits in the cantons.

In 2019, the OA-IA will assess the cantonal intelligence services. Each canton designates an authority to work with the FIS in order to implement the Intelligence Service Act and ensures that the FIS's assignments are carried out without delay.

## 5.5 Acceptance

In 2018, the OA-IA issued a total of 32 recommendations and 30 advisory notices. The Head of the DDPS accepted all the recommendations made by the OA-IA and instructed his services to implement them. Some recommendations and advisory notices were already implemented in the course of 2018.

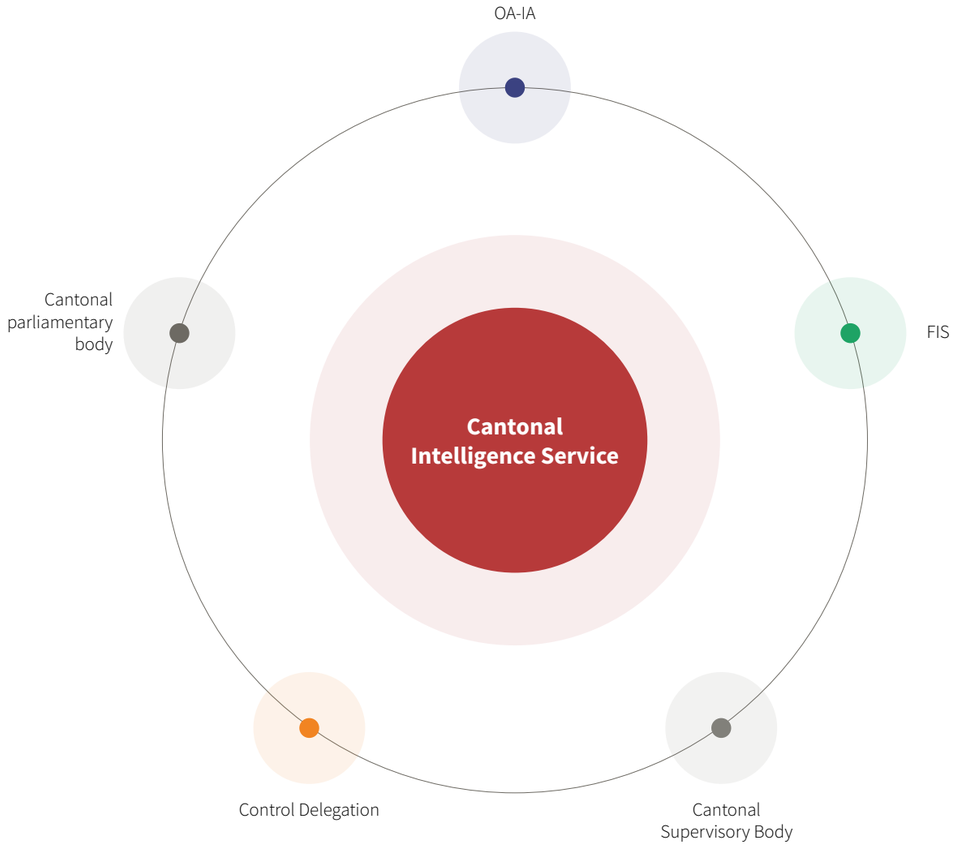
The OA-IA monitors the implementation of its recommendations. It will audit the implementation in each case and if need be conduct follow-up audits.

Without exception, the audit managers were received professionally and in a spirit of cooperation by all the agencies audited.

They were granted access wherever requested, including access to documents and information systems. The interviewees took the time required for the interviews and made themselves available for all the OA-IA's questions.



Supervision of the cantonal intelligence service






# 6. Coordination

## 6.1 Contacts with other bodies and agencies

The OA-IA held discussions in 2018 with a number of national agencies and other supervisory authorities. The coordination of oversight activities is a key assignment for the OA-IA.

**Control Delegation**

Parliament has delegated the oversight of the activities of the intelligence services to a joint committee, the Control Delegation (CDel), formed from the two control committees (CCs). The Control Delegation comprises three members each from the CC of the National Council and the CC of the Council of States.

The CDel invited the OA-IA 2018 to three hearings, on 16 May, 24 October and 20 November 2018. The OA-IA provided information at these hearings on matters including the structure and organisation of the OA-IA and the recruitment of its staff. In addition, the OA-IA presented its first audit reports together with the recommendations it had made to the members of the CDel, and answered the Delegation's questions. The OA-IA will continue to inform the CDel about its activities in the future.

**Council of States Security Policy Committee**

On 24 April 2018, the SA-IA was invited to a meeting with the Security Policy Committee of the Council of States (SPC-CS). In its talks with members of parliament, the Director of the SA-IA was able to present his objectives, provide an update on the development of the SA-IA, and explain the efforts being made to coordinate activities with other agencies.

**Federal Department of Defence, Civil Protection and Sport**

The Head of the Federal Department of Defence, Civil Protection and Sport DDPS, Guy Parmelin, and the Director of the OA-IA held three meetings in 2018. The OA-IA made itself available to Federal Councillor Parmelin on each occasion for questions about the audit reports and the individual advisory notices and recommendations. No use was made of the procedure for escalation to the Federal Council in the event of recommendations being rejected.

**Independent Control Authority for Communications Intelligence**

The Independent Control Authority for Communications Intelligence (CICA) is an agency within the Administration that reviews the legality and proportionality of intelligence service assignments involving long-term radio communications intelligence operations. Under the ISA, the CICA is also responsible for supervising the execution of approved assignments involving cable communications intelligence.

On 9 August, a meeting took place between the Director of the OA-IA and the president of the CICA. They discussed their areas of responsibility, the division of their roles and their activities. Talks covered in particular how to make the most of synergies between the supervisory bodies and to avoid duplication. Wherever necessary, supervisory and auditing activities are coordinated on a bilateral and informal basis.

### ➔ Intelligence gathering measures requiring approval (IGMRAs)

The Intelligence Service Act (ISA), which came into force in 2017, permits the FIS to use new information gathering measures, provided approval is obtained beforehand (intelligence gathering measures requiring approval (IGMRAs)). For example, several telecommunications connections belonging to the same person can be monitored, vehicles can be tracked and private premises can be searched. The new measures are possible in cases that carry a particularly high potential threat, e.g. in relation to terrorism, espionage, proliferation, attacks on critical infrastructure or safeguarding other important national interests. In each case, the Federal Administrative Court must approve these information gathering measures and they must be given clearance by the Head of the DDPS, who must also consult the Head of the DFA and the Head of the FDJP. They are subject to strict controls carried out by the Independent Oversight Authority for Intelligence Activities and the Control Delegation.

Contact with other bodies and agencies


**Swiss Federal Audit Office**

The Swiss Federal Audit Office (SFAO) monitors financial management not only in the Federal Administration but also in numerous semi-stated-owned and international organisations. On various occasions, the OA-IA discussed specific audit topics with the manager of Audit Area 1, which includes the FIS and AFIS.

**Federal Administrative Court**

Division I of the Federal Administrative Court decides on applications made by the FIS in relation to information gathering measures requiring approval (IGMRAs) and cable communications intelligence.

The exchange of experiences with this institution is important for the OA-IA, even though the court is not subject to its supervision. Accordingly, on 21 February 2018 a bilateral exchange of experiences took place.

**Supervisory Authority for the Office of the Attorney General**

The common ground between the intelligence service and the prosecution authorities is of vital importance to both partners in fulfilling their mandates. Right from the development phase of the OA-IA, questions about organisation, processes and possible synergies were an important matter. The Supervisory Authority for the Office of the Attorney General SA-OAG has been carrying out its supervisory activities since 2011. The SA-OAG and the OA-IA met on 28 November 2018 for a discussion, which they now plan to hold every year. The two supervisory authorities exchanged views on matters that they have in common and on their experiences.

**Post and Telecommunications Surveillance Service**

On 29 March 2018, the OA-IA had the opportunity to visit the Post and Telecommunications Surveillance Service (PTSS) and was able to gain a picture of its activities in situ. Information is often found in post and in telecommunications, which also includes the internet, that may be required in the investigation of serious crimes. The PTSS can carry out post and telecommunications surveillance operations on the order of the FIS.

**Enquiries from the public**

In 2018, the OA-IA received seven enquiries from the public, all of which it answered. The persons concerned felt worried or threatened by possible intelligence service activities or pointed out irregularities in connection with suspected intelligence activities.

The OA-IA can make use of information provided by private individuals in its audit activities; for example, it may check whether the activities described can be attributed to the FIS and if so, whether the FIS is acting lawfully. However, the OA-IA is not a complaints body and is not permitted to notify private individuals about any findings that it makes.



Members of the public can request the Federal Data Protection and Information Commissioner (FDPIC) for information on whether any data about private individuals is being lawfully processed and whether any refusal to provide information is justified.

## 6.2 Contact with international agencies

International exchange is also important for oversight bodies. International cooperation among services is part of the daily routine and is particularly close with partner services. The jurisdiction of supervisory bodies normally ends at their national borders, even though data and information are exchanged between intelligence services. There is no legal basis for or coordination of international cooperation between supervisory bodies. This makes it all the more important to have an exchange in relation to proven methods and possible measures. Progress was made with this in 2018, primarily by signing a joint declaration on the limits and possibilities of intelligence supervision involving several countries.

**Oversight Meetings in Copenhagen (19 June 2018) and Bern (22 October 2018)**

The meeting in Copenhagen was attended by representatives of the oversight authorities from Denmark, Belgium, Holland, Norway and Switzerland. Each supervisory authority made a brief presentation on the situation in its own country. In addition, progress was made on a joint declaration on the limits and possibilities of intelligence supervision involving several countries.

On 22 October 2018, the OA-IA invited the supervisory authorities from Denmark, Belgium, the Netherlands and Norway to approve and sign the joint declaration. All five authorities were satisfied with the text and the participating chairpersons signed the document. The joint declaration was published on 14 November on the OA-IA website.

There is a need to define the confidentiality threshold for cooperation in relation to supervisory activities.

**21 and 22 November 2018 Bilateral exchange between Belgium and the OA-IA**

On 21 and 22 November 2018, a meeting was held in Bern between the members of the OA-IA and a delegation from the standing committee for the oversight of intelligence and security services in Belgium (“Comité R”). The meeting involved presentations and discussions covering a variety of topics. After the two authorities introduced themselves and their intelligence service architectures, a discussion was held on legislative developments in the two countries – in particular with regard to information-gathering measures and methods. The issue of data protection in relation to intelligence services and the question of radio and cable communications intelligence were also considered. The DDPS intelligence service adviser, who had also been invited, gave a presentation on his role as a link between the Department and the FIS and the consequences of the entry into force of the ISA for the Department. At the end of the meeting, the Director of the OA-IA and the Chairman of the Comité R expressed their joint wish to intensify cooperation between the two authorities.

→ Cable communications intelligence

Cable communications intelligence involves the recording of signals transmitted from country to country on cable-based networks in order to gather information on security-related events abroad and to safeguard other important national interests.

“By exchanging views at an international level, we get confirmation that we are on the right track at a national level.”

From left to right: Harm Brouwer (Netherlands), Thomas Fritschi (Switzerland), Eldbjørg Løwer (Norway) and Serge Lypszyc (Belgium).

**07. December 2018 First meeting in Paris between the national bodies of European countries**

The French Commission nationale de contrôle des techniques de renseignement (CNCTR) and the Belgian commission pérmanente R invited the heads of European supervisory bodies for a meeting in Paris on 7 December. A total of 14 European countries took part. The aim of the event was to forge contacts and exchange experiences. The national supervisory bodies are structured very differently. In some cases, it is very difficult to compare their respective tasks, powers and resources. The event provided an opportunity to successfully consolidate cooperation with Belgium. A call to repeat the event was welcomed by all the participants. A practical problem is exchanging views on the content of intelligence activities, as for almost all the participants there is no legal basis for doing so. It is planned to improve the situation in this respect, in view of the increasing international cooperation between the services that are now acquainted – and thus also the increasing exchanges of data – for the benefit of the supervisory bodies.

Individual members of staff from the OA-IA also attended the following international events:

- 15/16 March 2018: Second symposium on the law applicable to intelligence services – Reform der Nachrichtendienste zwischen Vergesetzlichung und Internationalisierung, Berlin
- 14 Mai 2018: New Responsibility Foundation, Berlin: first workshop of the European Intelligence Oversight Network (EION)
- 5 June 2018: Meeting with the independent body / Karlsruhe[7]
- 17 September 2018: New Responsibility Foundation, Berlin: Democratic control of networks of intelligence services & security services

[7] The Independent Body is a three-person body in the German Federal Court of Justice that reviews the communications intelligence conducted abroad by the German Federal Intelligence Service with regard to its legality and necessity



# 7. A view from outside (carte blanche)

By their nature, many intelligence activities have to be carried out away from the public eye or indeed in secrecy. In order to protect sources and sovereign interests, transparency is only possible to a limited extent or is not possible at all. Although their aim is to protect the general public, intelligence activities regularly compromise the individual freedoms of people living in Switzerland. Although the OA-IA represents the interests of these people, it is also recurrently guided by the actual needs of the population as a whole. In this Annual Report, there should be a place for a view from outside. This year Dr. Salome Zimmermann has been given the carte blanche.

**Salome Zimmermann** (*1955), Dr of laws and attorney-at-law, President of Division I of the Federal Administrative Court in St. Gallen from 2015 to 2018. In this capacity, she was responsible for planning the approval procedure under the ISA and sat as a single judge in approval procedure cases from 1.9.2017. She began working at the Federal Administrative Court in 2005.

**Does more oversight necessarily mean better oversight?**

The ISA brought change not only to the intelligence service, but also to the supervision of intelligence service activities. The draft IntelSA simply assumed that there would be parliamentary oversight of the intelligence service;[8] the OA-IA was not included in the draft, which provided that the Department would supervise the intelligence services.[9] Yet from the very first debate, the Council of States Security Policy Committee proposed that an intelligence service supervisory body be created that would be autonomous and independent of the DDPS. The wording of the provisions on the OA-IA that are now in the IntelSA were added by the National Council Security Policy Committee.[10]

This Annual Report names the authorities that fulfil the tasks related to the supervision of intelligence activities and describes their spheres of activity. There are nine of these authorities. If one also counts the Federal Administrative Court, which decides on information gathering measures that require approval, then a total of ten agencies are involved in the supervision of the intelligence services. How are supervisory activities coordinated between all these authorities? For this is essential, in order to avoid duplication or indeed omissions. Duplication is undesirable on cost and efficiency grounds, while omissions can cause constitutional and political damage.

[8] Art. 77 draft IntelSA, see Dispatch to the Intelligence Service Act of 19 February 2014, BBl 2014 2105 ff.
[9] Art. 74 draft IntelSA
[10] In addition, the word ‘exclusively’ was removed from the article on parliamentary oversight, even though the OA-IA does not exercise any form of parliamentary oversight (see Art. 77 draft IntelSA and Art. 81 IntelSA)

The ISA states that the OA-IA should coordinate its activities with parliamentary oversight activities and with other federal and cantonal supervisory bodies.[11] The Ordinance on the Supervision of Intelligence Activities (OSIA)[12] specifies the details of this under the heading "Cooperation between supervisory bodies", stating that the OA-IA will be offered the documents relating to intelligence service activities that are given to the executive, the CDel and the Finance Delegation. In addition, it states that the annual report that the President of the relevant division of the Federal Administrative Court submits to the CDel will also be sent to the OA-IA.[13] Furthermore, the ordinance provides that the OA-IA and the CICA should coordinate their supervisory and auditing activities and provide each other with information on their activities.[14] The OA-IA, the CICA, the Swiss Federal Audit Office and the other federal and cantonal supervisory bodies are authorised to exchange information relevant to their supervisory and auditing activities.[15]

On the other hand, the parliamentary supervisory bodies have no statutory duty to coordinate their activities with those of the OA-IA.[16] Under the Parliament Act, the CDel exercises its powers of oversight selectively, placing the emphasis on legality, expediency and effectiveness.[17] This means that it applies the same criteria that the OA-IA applies in its activities.[18] Should the same things be audited twice? How could a useful distinction be made between these two supervisory activities?

Effective overisght is based on a risk analysis. The risks that the oversight of the intelligence service is intended to counter result in particular from the technologies used, its federal organisation, international cooperation, but also from the broad scope for action that the intelligence service must be given in order to fulfil its mandate – quite apart from the fact that its activities take place far from the public eye. It should also be borne in mind that political decisions have to be made, especially when fighting terrorism and conducting counter-espionage.[19]

[11] Art. 78 para. 2 IntelSA
[12] SR 121.3
[13] Art. 5 OSIA
[14] Art. 14 para. 1 – 3 OSIA
[15] Art. 14 para. 4 OSIA
[16] In the following remarks, I restrict myself to a possible demarcation of the supervisory activities carried out by the CDel and the OA-IA.
[17] Art. 52 para. 2 ParlA
[18] Art. 78 para. 1 IntelSA
[19] The IntelSA takes account of this in that for intelligence gathering measures requiring approval and cable surveillance, it provides not only for the approval procedure by the Federal Administrative Court but also for obtaining clearance from the Head of the DDPS.



The OA-IA and CDel have quite different skills and powers that place limits on effective checks and must be used as a basis for demarcating their supervisory activities. The OA-IA has staff with broad expertise and experience. It conducts its audits based on a specific programme that is drawn up every year in advance and is available to the public. Likewise, its annual report is published. As a result, it is particularly suited to conducting checks in relation to legality and effectiveness. In addition, as a highly competent newcomer, it can efficiently relieve the burden on the CDel, which has supervised the intelligence service for many years. On the other hand, the CDel's key activity lies where the OA-IA reaches its limits, i.e. wherever authorities other than the intelligence services are active in the field of national security; and in areas that must remain secret because if they came to the knowledge of unauthorised persons this could cause serious damage to national interests.[20] The OA-IA is not permitted to look into the activities of fedpol, because fedpol is not an intelligence service authority. Furthermore, it has no powers of any kind in relation to political judgements. This remains the CDel's core business, because it exercises general oversight over state activities in relation to national security and the intelligence services. And it examines state action in areas that are subject to secrecy.[21] Accordingly, it is only the CDel that can investigate the interaction between the intelligence service and the prosecution authorities and conduct analyses based on political criteria in order to establish political responsibility. This demarcation of roles will take time to establish itself. It requires a continuous dialogue and mutual trust.

The ISA has introduced effective new control mechanisms that apply to the intelligence service and its activities, such as requiring court approval for certain information gathering measures. It is to be hoped that the numerous other supervisory authorities not only conduct a greater number of checks, but achieve more precise supervision in other areas thanks to their expertise and the coordination of their activities.

[20] Art. 53 para. 2 ParlA
[21] Art. 53 para. 2 ParlA

# 8. Key figures as of 31.12.2018

## Staff

| | |
|---|---|
| 1.1.2018 | **4** |
| 31.12.2018 | **9** |
| Departures | **1** |

## Audits

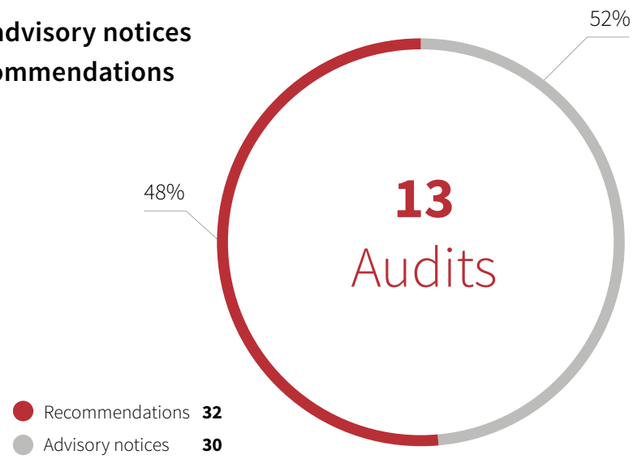
| | |
|---|---|
| Planned audits | **12** |
| Unannounced audits | **0** |
| Completed audits | **13** |

## Number of interviews conducted in 2018 **72**

## Budgeted workforce

**10 full-time positions**

## Audits, advisory notices and recommendations






# 9. Annex

## 9.1 2018 Audit Plan

| No | Name of audit | Agency audited |
|---|---|---|
| **18-1** | Overview of the FIS data landscape and content of the residual data memory | FIS |
| **18-2** | Electronic work aids in the workplace | FIS |
| **18-3** | Compliance with requirements when implementing information gathering measures requiring approval (IGMRAs) and cable communications intelligence assignments | FIS, EOC |
| **18-4** | Follow-up audit on FIS readiness in relation to the ISA | FIS |
| **18-5** | Operations management / Management cycle | FIS |
| **18-6** | Recruitment and screening of human sources (Art. 15 ISA) | FIS |
| **18-7** | Composition of the organisation and assignments carried out by the intelligence units in the Armed Forces | AFIS |
| **18-8** | Survey and evaluation of the implementation of the cantonal audit mandate / Conference with cantonal supervisory authorities | Cantons |
| **18-9** | Overview of the EOC data landscape and review of the selectors in the system | EOC |
| **18-10** | Overview of the measures to reduce risks in the FIS (including FIS checks on the CIS) | FIS |
| **18-11** | Overview of the measures to reduce risks in the MIS | MIS |
| **18-12** | Overview of the measures to reduce risks in the EOC | EOC |

## 9.2 List of abbreviations

**AFD** Armed Forces Development Programme

**AFIS** Armed Forces Intelligence Service

**Art.** Article

**BND** German Federal Intelligence Service

**CC** Control Committee

**CDel** Control Delegation

**CIS** Cantonal intelligence service

**CNCTR** Commission nationale de contrôle des techniques de renseignement (France)

**CSBs** Cantonal supervisory bodies

**DDPS** Federal Department of Defence, Civil Protection and Sport

**DPA** Federal Data Protection Act (SR 235.1; DPA)

**EION** European Intelligence Oversight Network

**EOC** Electronic Operations Centre

**FDPIC** Federal Data Protection and Information Commissioner

**FFA** Federal Finance Administration

**FinDel** Finance Delegation

**FIS** Federal Intelligence Service

**GS** General Secretariat

**IAFP** Integrated Task and Financial Plan

**IASA** Integrated analysis system of the FIS

**IntelSO** Ordinance on the Intelligence Service (Intelligence Service Ordinance, SR 121.1; IntelSO)

**IR** Internal revision

**ISA** Federal Act on the Intelligence Service (Intelligence Service Act, SR 121; ISA)

**ISFP** Information security and facility protection

**ISMS** Information Security Management System

**ISSO-FIS** Ordinance on the Federal Intelligence Service Information and Storage Systems (SR 121.2; ISSO-FIS)

**MIS** Military Intelligence Service

**NSA** National Security Agency (foreign intelligence service the United States of America)

**O-AFIS** Ordinance on the Armed Forces Intelligence Service (SR 510.291; O-AFIS)

**OA-IA** Independent Oversight Authority for Intelligence Activities

**SA-OAG** Supervisory Authority for the Office of the Attorney General

**SFAO** Swiss Federal Audit Office

**SiA** Federal Council Security Committee

**SPC** Security Policy Committee

**SR** Classified Compilation of Federal Legislation

**Independent Oversight Authority**
**for Intelligence Activities**
Maulbeerstrasse 9, 3003 Bern
Phone +41 58 464 20 75
www.ab-nd.admin.ch