Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Independent Oversight Authority for Intelligence Activities

Annual Report 2021
of the Independent Oversight Authority for Intelligence Activities OA-IA

1. Summary

Three events shaped the activities of the Independent Oversight Authority for Intelligence Activities (OA-IA) in 2021: the departure of the director of the Federal Intelligence Service (FIS); the marked increase in the number of reports concerning dissatisfied FIS employees; and staff changes at the OA-IA itself, including the departure of its director, Thomas Fritschi, after nearly five years at the helm. Despite these developments, the OA-IA fulfilled its main mandate, i.e. the oversight of intelligence activities.

In 2021, the OA-IA carried out audits in the following areas:

- Strategy and planning – 1 audit
- Organisation – 3 audits
- Cooperation – 8 audits
- Information gathering – 4 audits
- Data processing and archiving – 2 audits

A total of 18 audits were carried out and completed. Compared with the last few years, the number of recommendations made by the OA-IA has fallen significantly. This can be attributed on the one hand to improvements already achieved by implementing past OA-IA recommendations. On the other hand, the OA-IA, having spent the early years largely gaining an overview of the various intelligence activities, is now performing more in-depth audits. This makes formulating level-appropriate recommendations more demanding and therefore fewer in number.

In line with its risk assessment, the OA-IA focused its oversight activities in 2021 on the FIS, where it carried out 17 audits.

The OA-IA used considerable resources examining cooperation between the FIS and the cantonal intelligence services (CIS) and assessing the protection of critical infrastructures through cyber defence and information gathering through human sources (human intelligence, HUMINT). It also conducted an extraordinary, extensive audit in the area of HUMINT, which was not originally on the 2021 audit plan. The FIS addressed those areas requiring improvement. The long transition period after the departure of its director and staff dissatisfaction have been challenging for the FIS. It achieved good marks with respect to cooperation with the CIS; this close cooperation makes a major contribution to Switzerland's internal security. In the cyber field, the FIS reviewed its practice with respect to information gathering and informed the OA-IA regularly and in detail about its progress so that a decision could be made on whether to conduct a full audit.

The OA-IA reviewed cyber defence at the Electronic Operations Centre (EOC). The audit showed that the necessary competences for protecting critical infrastructure at the FIS and EOC have been established and the two bodies cooperate well. In addition, the OA-IA participated as an observer in the meetings of the Independent Control Authority for Radio and Cable Communications Intelligence (ICA).

The OA-IA carried out an audit on data protection at the Military Intelligence Service (MIS). Although the MIS processes personal data, this is not the focus of its work; its legal mandate is primarily to gather information on foreign countries. The OA-IA did not identify anything that led it to doubt the lawfulness of personal data processing at the MIS.

In addition, the OA-IA and the cantonal oversight authorities met at a conference to cultivate and strengthen relations.

The 2021 Annual Report was prepared in consultation with the DDPS and the Control Delegation of both the National Council and the Council of States from 14 to 27 February 2022. Where feedback indicated formal or material errors in the report or interests worthy of protection that precluded publication of certain parts, these were taken into account.

Conclusion

The OA-IA formulated 18 recommendations regarding the 18 audits conducted. Implementing these recommendations will reduce existing risks in intelligence activities and improve their effectiveness.

Staff insecurity at the FIS had a negative effect on its intelligence activities in the year under review. Although it has taken initial steps to improve the situation, these are unlikely to be sufficient to remedy the situation in the long term. The FIS's structures and process must be examined and if necessary adapted. This will create stability in the long term, thus reducing risks. To achieve this, the FIS requires the support of the DDPS. The falling number of OA-IA recommendations indicates that existing risks in intelligence activities have either been eliminated or at least minimised.

Based on the OA-IA's risk assessment, the audit of the two military intelligence bodies, the MIS and the EOC, was less comprehensive and no recommendations had to be made for them. It remains to be seen how the EOC will be integrated into the Armed Forces Cyber Command in the future.

2. Table of contents

3. Personal

"The OA-IA provides a range of checks and balances in the field of intelligence services."

Thomas Fritschi

Thomas Fritschi, OA-IA Director

The COVID-19 pandemic and the consequent drift towards social division, the power politics of individual states and our vulnerability to cyberattacks make us aware of how fragile our security is and how important prevention and situation assessment are for political decision makers. In these increasingly uncertain and difficult times, the need for secure information and facts has become even greater. The intelligence services are challenged, and so is their oversight.

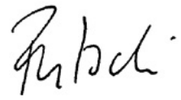
In the year under review, we continued to carry out our oversight activities on the basis of our risk assessment and in line with current developments. Our recommendations have declined significantly in number. This is due to the fact that improvements have already been achieved in recent years and to the fact that we are focusing more on the basic challenges that arise from intelligence work in a democratic state. This requires audits to be more comprehensive and places higher demands on formulating recommendations to the appropriate level. An audit of human source management and an in-depth review of incidents concerning the FIS's cyber unit proved to be particularly demanding.

Our audit of the FIS focused on its organisation, which was put to the test by the surprise departure of its director. Then, in mid-year, reports concerning dissatisfied employees emerged in the press. A change of culture and a review of structures and processes are therefore necessary. Implementing change will be the responsibility of the new director rather than of the OA-IA.

In addition to reporting on our auditing activities and on FIS-internal developments, we take a look in greater detail in this report at the topic of information systems, including the question of data protection. We are delighted to have Federal Data Protection and Information Commissioner Adrian Lobsiger as editor of the 'A view from outside' chapter. Dr Lobsiger is a proven specialist in this field.

This is my last annual report. I look back on almost five years of gratifying and constructive work in a highly sensitive and demanding field. The OA-IA provides a range of checks and balances with respect to the greater powers granted to the FIS in 2017 and to an intelligence service that is continually expanding. The structure and development of the OA-IA can meet this challenge, and its independence is noted and respected. Cooperation and coordination with other federal and cantonal oversight bodies are established. It is to be hoped that a dialogue with the Control Delegation, which is responsible for parliamentary oversight, may take place in the future.

The OA-IA is indispensable and enhances confidence in intelligence activities. I would like to thank you for the trust you have placed in me over the past years and I hope you enjoy reading this report.



Thomas Fritschi, OA-IA Director

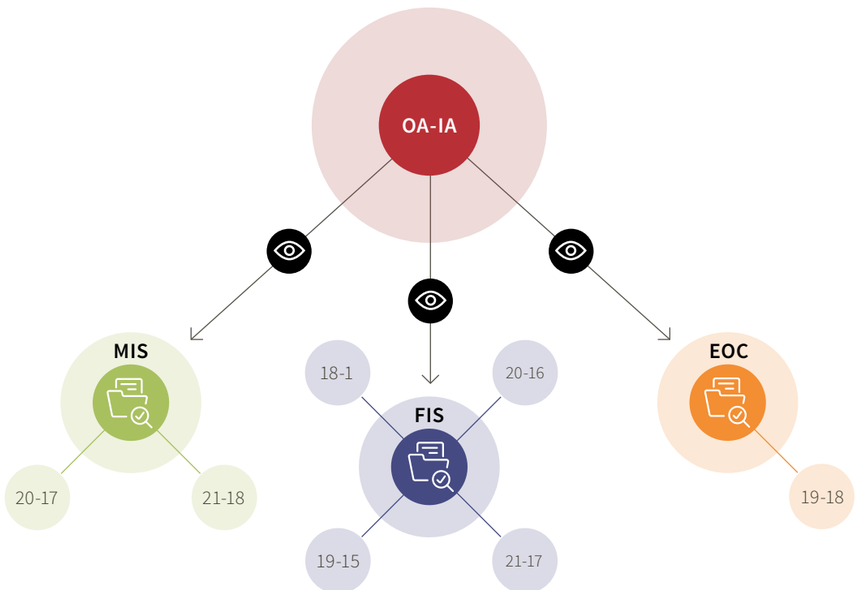
4. Information systems

"Each year the OA-IA reviews a number of data processing operations or information systems."

One of the key tasks of the Swiss intelligence services is to gather information regarding certain tasks prescribed by law and make it available as soon as possible to domestic and foreign security services and military and political decision makers in the form of intelligence reports. The purpose of this information gathering is to assess the prevailing threat situation so that appropriate preventive measures can be taken at national and international level.

Information that is no longer required by the intelligence services to fulfil their tasks and whose retention period has expired is passed on to the Swiss Federal Archives (SFA). If the SFA considers the information not worth archiving, it must be destroyed.

The intelligence services operate a network of information systems that process data, from its procurement to deletion. The applicable laws contain a number of regulations on data retention. As this area is important for the intelligence services, the OA-IA has defined two specific areas in its audit plan: data processing and archiving. Each year the OA-IA reviews a number of data processing operations or information systems. This year our report focuses on information systems.



4.1 Information systems audited by the OA-IA to date

To date, the OA-IA has audited the following FIS information systems:

Audit	Purpose	Year/Source
18-1 Overview of the FIS data landscape and content of the residual data memory	Article 47 of the Federal Act on the Intelligence Service (Intelligence Service Act, IntelSA)[1] lists the information systems operated by the FIS. The information systems are further regulated at the ordinance level.[2] The OA-IA used this audit to obtain an overview of all the FIS's information systems. The audit served as a basis for future audits. As the residual data memory can contain data that cannot be assigned to any other information system, the OA-IA inspected the system in order to determine what kind of data it contained.	2018 (2018 Annual Report, page 13)
19-15 Operation, content and use of the information systems GEVER FIS[3], BURAUT data storage[4], and SiLAN[5] data storage (temporary evaluations)	In 2012, the FIS introduced a business management system containing both administrative and intelligence data. All FIS staff have access to it. In view of the kind of data processed and the large number of authorised users, the OA-IA chose to perform an initial in-depth audit of a system.	2019 (2019 Annual Report, page 23 ff.)
20-16 Operation, content and use of the IASA information system[6]	IASA comprises three key intelligence information systems and is the FIS's main work instrument, which was the reason for the OA-IA audit	2020 (2020 Annual Report, page 23 ff.)
21-17 Selected FIS information system (Quattro P)	This information system stores and processes a large volume of data on the [travel] movements of foreign nationals. The OA-IA chose to audit Quattro P because it contains a large volume of personal data and because the system is used for the FIS's facial recognition system.	2021 (2021 Annual Report, page 21 ff.)

1 SR 121
2 Ordinance on the Federal Intelligence Service Information and Storage Systems (ISSO-FIS; SR 121.2)
3 Electronic records and process management system of the FIS
4 Data storage system of the FIS
5 Secure network of the FIS
6 Integral analysis system of the FIS

To date, the OA-IA has performed an audit of the following MIS information systems:

Audit	Purpose	Year/Source
20-17 MIS information system landscape	The OA-IA used the audit results to gain an understanding of the information systems and to plan further audits.	2020 (this topic was not dealt with specifically in the annual report, but a summary is available on the OA-IA website.)
21-18 Data protection within the MIS	The MIS processes personal data although this is not the main focus of its activities. The OA-IA therefore inspected the data protection aspects of its activities in certain information systems.	2021 (2021 Annual Report, page 24 ff.)

To date, the OA-IA has audited the following EOC information systems:

Audit	Purpose	Year/Source
19-18 EOC information system landscape	The purpose of this audit was to gain an overview of the EOC information systems landscape and to serve as a starting point for further audits. There is no specific legal base governing the EOC's information systems; their operation is regulated in various acts and ordinances.	2019 (2019 Annual Report, page 27)

Besides examining specific information systems, the OA-IA has also carried out audits in the area of data processing and archiving, amounting to ten additional audits since the beginning of its oversight activities. Thus, since taking up its duties, the OA-IA has carried out sixteen audits of the information systems of the intelligence services and of data processing in these systems. The findings of these audits are presented below.

"The relevant legal bases for operating the FIS's information systems are more detailed and more transparent than the legal bases for operating the MIS and EOC systems."

4.2 What challenges and opportunities does the OA-IA see in connection with the audited information systems?

4.2.1 Legal base of intelligence information systems

The information systems of the FIS, MIS and EOC do not have the same legal bases. The relevant legal bases for operating the FIS's information systems are more detailed and more transparent than the legal bases for operating the MIS and EOC systems. These clear legal provisions make auditing the lawfulness of the FIS's information systems easier. The OA-IA is therefore working to ensure clearer and more specific legal bases for the MIS and EOC information systems in the future.

4.2.2 Access by the OA-IA to intelligence information systems

During an audit, the OA-IA auditors have direct and time-limited access only to the information systems of the FIS. They also have permanent access to the FIS's electronic records and process management system. This ready access facilitates auditing activities because the OA-IA can obtain the required documents independently. This is not the case at the MIS or the EOC, where the OA-IA auditors must be shown the systems or must organise on-site access, making the independent processing of random samples from these systems difficult.

4.2.3 Addressees of the recommendations and their implementation

The EOC and the MIS are relatively small organisational units within the Armed Forces and the scope for individual information systems tailored to their specific needs is therefore limited. This poses challenges for the OA-IA when formulating practicable recommendations, because the recommendations may only apply to the intelligence services and not to other sections of the Armed Forces. However, recommendations in this area nearly never only concern the MIS or the EOC, but often have intersections overlap to the whole Armed Forces.

4.2.4 Focus of the OA-IA's information systems audits

Access management and deletion of data – the information systems of the FIS

Our audits of the FIS information systems focus particularly on compliance with data retention periods as well as lawful and expedient access management. The FIS has more than ten different retention periods for the data in its systems, ranging from 6 months to 45 years. Compliance with these periods is largely ensured by automatic deletion programs. The OA-IA carries out random checks in the systems to verify deletion.

Access management poses major challenges for the FIS. For information and data protection reasons, staff may only access the data they require for their work. After an internal job change, or on joining or leaving the FIS, authorisations must be updated promptly. The FIS has installed dedicated processes for this purpose, and the OA-IA conducts random checks in the information systems to verify authorisations. It can also request staff to demonstrate systems access at their workstation.

Time delay in processing information

It is important for the intelligence services that the information they gather or receive is entered into the appropriate systems as quickly as possible. For reasons of information security, procured data is sometimes first stored in specially protected temporary files. Only then is it transferred to the information systems to which staff have access for their analyses and for use in their reports. Moreover, information must sometimes be anonymised before being entered in a system. The OA-IA therefore pays close attention to examining these processes.

“Although new technologies can pose risks to our country’s security, they can also have a positive impact on the work of the intelligence services.”

4.3 Future developments

The intelligence services must be in a position to anticipate societal and technological changes that negatively impact the security of Switzerland. Although new technologies can pose risks to our country’s security, they can also have a positive impact on the work of the intelligence services. The FIS’s cross-system search engine, for example, has greatly facilitated the work of its staff since its introduction six years ago.

All three services keep track of technological developments and make use of them in their intelligence activities. For example, a new facial recognition system allows the FIS to pull up an overview of facial images in its systems (see page 18 ff.). The MIS, for its part, is increasingly promoting satellite imagery analysis. And the EOC is addressing the question of how decreasing radio traffic – a result of the emergence of new communication technologies – can be monitored using other technical means.

4.4 New data management: Impact on the Intelligence Service Act

Legislation on data management generally uses the term ‘information system’. This is also the case in the Intelligence Service Act (IntelSA). Article 47 IntelSA lists the various FIS information systems. The dispatch to the IntelSA states that the FIS should file the information it collects or receives in a network of information systems according to topic, source or sensitivity.[7]

However, linking the term ‘information system’ to the intended purpose of data processing in legislation may no longer correspond to modern concepts of data management. The new Data Protection Act, for example, does not use the term ‘collection of data’. The reason given for this is that, thanks to new technologies, data is used like a collection of data even if it is not stored centrally.[8]

The draft revision of the IntelSA requires an amendment to the legal provisions governing the FIS’s information systems. The term ‘information’ should be replaced by the term ‘data’. Data should be categorised according to the legal requirements. The content of these categories should correspond approximately to those of the information systems described in the IntelSA.

[7] BBl 2014 2106

[8] BBl 2017 7023

5. Oversight activities

In a practice introduced last year, the OA-IA no longer includes every audit carried out in its annual report. Instead, it sets priorities, providing detailed information on some audits and no information on others. However, a summary of the results of all its audits is available on the OA-IA website.[9]

5.1 Audit plan

Each year, the OA-IA draws up a risk-based audit plan[10] for the following areas:

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

In 2021 the OA-IA planned and carried out a total of 18 audits. In addition, it carried out audit 20-3 'Allocation of powers and responsibilities between FISA[11] and the MIS', originally scheduled for 2020, as well as an extraordinary audit of HUMINT. However, it decided not to perform audit 20-1 'Change management' or audit 21-3 'FIS security' because a temporary lack of personnel resources or a significant change in circumstances between the planning and realisation stages of the audits meant they no longer made sense. However, individual aspects of these audits were either included in other audits or will be taken into account in future ones. Audit 21-16 'Telecommunication Services' was launched in 2022.

Based on current events and developments, the OA-IA also conducted three short-term individual assessments in view of a possible audit. Some of the findings from these assessments have been integrated into ongoing or future audits.

5.2 Audits conducted in 2021

5.2.1 Strategy and planning

In the area 'Strategy and planning', topics are examined that concern the short-, medium- and long-term strategic planning of Switzerland's intelligence services and their objectives. In 2021, the following audit was carried out in this area:

- **21-1 Deployment of FIS employees in Swiss representations abroad (FIS)**

This was a follow-up audit to audit 19-2 'Management of intelligence data between the defence attaché and the FIS'. It was aimed at examining how the recommendation from that audit had been implemented. The audit is described in chapter 5.4 of this report, under 'Controlling'.

5.2.2 Organisation

In the area 'Organisation', the OA-IA examines whether structures and processes within the intelligence services are suitable for fulfilling their legal mandate lawfully, expediently and effectively.

In 2021, the OA-IA carried out audit 20-3 'Allocation of powers and responsibilities between FISA and the MIS ', which had been scheduled for the previous year. The findings of the audit are presented in this report. The following audits were also planned for 2021:

- **21-2 Critical infrastructure protection/cyber defence (FIS/EOC)**
- 21-3 FIS Security(FIS)
- **21-4 Violent right-wing extremism (FIS)**

Audit 21-3 'FIS Security' was not carried out.

[9] https://www.ab-nd.admin.ch/en/pruefplan-und-pruefberichte.html
[10] See the OA-IA's 2020 Annual Report, page 9.
[11] FIS Evaluation Division

20-3 Allocation of powers and responsibilities between FISA[12] and the MIS (FIS/MIS)

The audit focused mainly on the question of whether there was a sufficient distinction between the intelligence products of the FIS and the MIS. The audit also looked at whether, in instances where they overlap, potential for synergy was being sufficiently used, for example by sharing expertise. The audit had originally been planned for 2020, but was then postponed because of a reorganisation of the FIS Evaluation Division. The audit was therefore launched in September 2021. The OA-IA conducted an in-depth analysis of the two services' intelligence reports and cooperation, taking into account their basic mandates and the cooperation agreement between them. The OA-IA found that there are only a few overlapping areas in their evaluation activities.

To prevent duplication there is a regular, partly formalised, exchange between the respective FIS and MIS departments. They inform each other about what topics are in the pipeline and share their intelligence products. This exchange of information is also reflected in the reports themselves, which tend to complement rather repeat each other when reporting on common areas of interest; reports often convey different perspectives despite the same starting point. The OA-IA therefore concluded that the distinction between the areas evaluated by the FIS and MIS was expedient and effective.

21-2 Critical infrastructure protection/cyber defence (FIS/EOC)

In its 'Switzerland's Security 2021' situation report, the FIS noted an increased vulnerability to cyberattacks as a result of greater digitalisation during the COVID-19 pandemic. Swiss companies providing equipment and specialised services for critical infrastructure operators in Switzerland and abroad are interesting targets also for state-sponsored attacks. The FIS believes that classic cyberattacks, cyber espionage, cyber sabotage and cyber terrorism directly targeting critical infrastructures make up only a small proportion of the overall cyber threats identified. Critical infrastructures in Switzerland have not been a direct target of attack as yet. Nonetheless, the sabotage of critical infrastructures is considered to have the greatest potential damage because infrastructure services, for example electricity or telecommunications, are of key importance for the functioning of society.

[12] FIS Evaluation Division

Based on these undisputed risks, the OA-IA examined whether the FIS and the EOC have sufficient powers and capacity, both in terms of quality and quantity, to gather the necessary information[13] in order to disrupt, prevent or slow down potential attacks on critical infrastructures.[14]

The cyber division at the FIS (CYBER FIS), the Reporting and Analysis Centre for Information Assurance (MELANI OIC[15]) and parts of the Armed Forces are the key actors for countering cyber threats. They are integrated into a complex, interdepartmental organisational structure whose objective is to protect critical infrastructures and defend against cyberattack. The main task of the FIS, together with the EOC, is to identify and categorise cyberattacks through intelligence means. The FIS also supports critical infrastructure operators with updates on the current cyber situation and draws on the resources of the EOC for a technical analysis of cyber threats.

CYBER FIS is responsible for operative and technical analyses. Similarly, the EOC has a Cyber Threat Intelligence (CTI) unit in the field of Cyber Network Operations (CNO), which analyses cyber threats. CYBER FIS is especially important for dealing with security-related incidents involving a foreign state; its scope of tasks does not include acts of cybercrime.

If a request by the FIS to take action against an aggressor according to Article 37 paragraph 1 IntelSA is approved, the FIS instructs the EOC to carry out the counter-attack because it does not have its own resources for doing so; according to the cyber strategy of the DDPS, this is the task of the Armed Forces. The Joint Cyber Technical Analysis Center (JCTAC) is a platform for cooperation that goes beyond the client-contractor relationship: it is not a new organisational unit, but rather a form of cooperation between FIS and EOC staff for the purpose of conducting joint technical analyses of cyber threats.

The audit showed that the FIS and the EOC have sufficient powers and capacity, and that both services work collaboratively.

Individual inquiry concerning CYBER FIS

Since May 2021, the OA-IA has been aware of irregularities in the CYBER FIS division and has closely monitored the resulting internal enquiries and posed follow-up questions where necessary. Generally, we agree with the approach taken by the FIS and the DDPS. The question of criminal liability is of great importance to us and we will therefore continue to closely monitor further developments and exert influence where necessary. So far, we have not seen any additional benefit in conducting our own further going enquiries or an audit.

21-4 Violent right-wing extremism (FIS)

The FIS is responsible for gathering and processing information for the early recognition and prevention of threats to Switzerland's internal and external security. This includes threats from violent extremism.[16]

The FIS and its activities in the field of violent right-wing extremism – just one area of violent extremism – have been repeatedly questioned and criticised by various sides. One criticism is that the FIS turns a blind eye to violent right-wing extremism and does not take the issue seriously enough.[17]

[13] Art. 6 para. 1 let. a No 4 IntelSA
[14] Art. 37 para. 1 IntelSA
[15] Operation Information Center at MELANI

[16] Art. 6 para. 1 let. a No 5 IntelSA
[17] For example, Postulate 02.3059; Postulate 17.3831; Question Time/Question 9.5677; Question Time/Question 21.7312; Die braune Gefahr – Die Schweiz ist keine Insel, Swiss Broadcasting Company (SRF), 12 May 2019; Wie neutral ist unsere Polizei?, in the 'Walliser Bote' newspaper, 23 July 2020; Geheimdienst soll Rechtsextreme ins Visier nehmen, in the 'Zeitung für die Region Basel' newspaper, 25 May 2021.

"Distinguishing between data processing that is allowed and desired or prohibited poses major challenges for the FIS employees."

A further, repeated accusation is that it gathers information on political activities unlawfully.[18]

In its 'Switzerland's Security 2020' situation report, the FIS concluded that members of right-wing extremist groups exercise restraint in their use of violence. The greatest risk of a right-wing extremist-motivated attack in Switzerland, the report said, is from lone actors with right-wing extremist views but with no firm attachment to established violent extremist groups. In its 2021 situation report, the FIS notes that the right-wing extremist scene has a considerable threat potential, but although existing groups have been dissolved and newly formed, there was only one violent incident that year.

The purpose of audit 21-4 was to examine whether the FIS has suitable strategies and processes in the field of right-wing extremism, whether these strategies and processes are implemented effectively and whether information is managed lawfully. The audit found that the FIS has a range of strategies and processes for dealing with right-wing extremism.

The FIS is not permitted to gather or process any information relating to political activities or the exercise of freedom of speech, assembly or association in Switzerland. This ban is known in German as the Datenbearbeitungsschranke (ban on data processing).[19]

On the other hand, the FIS is supposed to identify at an early stage dangers from violent right-wing extremism that pose a threat to Switzerland's internal and external security. Distinguishing between data processing that is allowed and desired or prohibited poses major challenges for the FIS employees. They have to deal with several demarcation questions in the course of their daily work, for example:

- What is the difference between extremism, violent extremism and terrorism?
- What is the exact definition of extremism,[20] i.e. when is a violent extremist act committed, incited or endorsed?[21]
- When is an occurrence a violent extremist act (and therefore may be addressed by the FIS) and when is it a political activity or the expression of freedom of speech, assembly or association (and therefore may not be addressed by the FIS)?[22]
- When can the FIS nonetheless process information relating to political activities or the exercise of freedom of speech, assembly or association in Switzerland because there is clear evidence that a person is exercising these rights and freedoms in order to plan or commit violent extremist act?[23]

Based on these questions and considerations, the FIS has developed various instruments to help its employees with their daily tasks. For example, it has established a collection of case studies and decisions based on these cases in order to help its employees to reach decisions in similar cases in the future.

One method of complying with the above-mentioned data processing ban is to anonymise information. According to the law, information that is gathered although not permitted and that concerns political activities or the exercise of freedom of expression, assembly or association in Switzerland must be anonymised. In audit 21-4, the OA-IA identified internal inconsistencies regarding the anonymization of reports and messages in relation to the data processing ban.

[18] For example, Parliamentary Procedural Request 19.3868; Geheimdienst überwacht Menschenrechtsorganisation seit 15 Jahren, Netzpolitik.org, 10 August 2021
[19] Art. 5 para. 5 IntelSA

[20] Art. 6 para. 1 let. a No 5 IntelSA
[21] Art. 19 para. 2 let. e IntelSA
[22] Art. 5 para. 5 IntelSA
[23] Art. 5 para. 6 IntelSA

"The FIS must ensure the lawful implementation of the IntelSA both in the FIS and the CIS through appropriate quality assurance and control measures."

Another important instrument in the daily work of the FIS staff is the watch list. This is a political control instrument of the Federal Council, which approves the list annually. The list contains the names of organisations and groups that are reasonably assumed to pose a threat to the internal or external security of Switzerland[24] and to which the data processing ban does not apply.[25]

In audit 21-4, the OA-IA examined whether the procedure used by the FIS for determining what right-wing extremist organisations are included on the watch list[26] is expedient. Based on random samples the OA-IA analysed the FIS's methods and judged them to be expedient.

Nor did the OA-AI find any irregularities, based on random samples, with regard to the lawfulness of information management. It interviewed third parties to verify the effectiveness of reporting and of information forwarded to them on right-wing extremism. The interviewees confirmed that the information they received from the FIS was generally effective.

5.2.3 Cooperation

This audit area covers national and international cooperation among intelligence services. The cantonal intelligence services (CIS) are an annual focal point of the OA-IA's audits. These audits are summarised below.

The OA-IA conducted the following audits in 2021:

- **21-5 FIS quality assurance within the Cantonal Intelligence Services (CIS) (FIS)**
- **21-6 Audit of the CIS Basel-Stadt (FIS/CIS)**
- **21-7 Audit of the CIS Basel-Landschaft (FIS/CIS)**
- **21-8 Audit of the CIS Appenzell Ausserrhoden (FIS/CIS)**
- **21-9 Audit of the CIS Appenzell Innerrhoden (FIS/CIS)**
- **21-10 Audit of the CIS Aargau (FIS/CIS)**
- **21-11 Audit of the CIS Vaud (FIS/CIS)**
- **21-12 Audit of the CIS Neuchâtel (FIS/CIS)**

21-5 FIS quality assurance within the Cantonal Intelligence Services (CIS/FIS)

Quality assurance is a risk-reducing measure. In addition to the regular audits of the cantonal intelligence services (CIS), the OA-IA also examined whether the measure had a risk-reducing impact on the CIS. This can ensure a well-functioning oversight of the CIS in cooperation with the OA-IA. Reliable and manageable quality assurance is important for the quality of the data and information of the FIS and of the CIS. The FIS must therefore ensure the lawful implementation of the IntelSA both in the FIS and the CIS through appropriate quality assurance and control measures. The FIS's quality assurance office (QS FIS) in the Cyber Information Management division is responsible for this task.

At least once a year, the QS FIS carries out random checks to verify the lawfulness, expediency, effectiveness and accuracy of data processing in all of the FIS's information systems. For this purpose, it draws up a control plan and – amongst other things – periodically checks CIS reports for their relevance and accuracy. It also deletes data from preliminary inquiries which was recorded more than five years previously and deletes data on the request of the CIS. In addition, it provides internal training on data protection matters.

The QS FIS always chooses the same procedure for carrying out random CIS checks. The individual steps in this procedure are scheduled with deadlines and assigned to the QS FIS staff. The individual steps include the allocation of the assignment, the collection of statistical data according to identical specifications, a questionnaire based on the statistics collected, the opinion of the CIS on the questionnaire and the final report. The final report is submitted to the FIS management for consultation and is then approved by the FIS directorate. The CIS receive the final report in this last step and the QS FIS monitors the implementation of its recommendations, if any. By involving the FIS management and the FIS directorate in the procedure, the report and recommendations receive the necessary weight vis-à-vis the CIS.

The QS FIS implements its CIS control mandate expediently and effectively. This is demonstrated, for example, by the fact that the QS FIS has developed a process for random sampling that guarantees sampling is always carried out in the same way and is based on identical procedures. The OA-IA confirmed this by carrying out two random checks. Clear internal mandates and a consistent dual-control procedure ensure that the controls are carried out efficiently and that potential risks are identified.

The QS FIS carries out its CIS control activities expediently and effectively by coordinating these activities internally and with the OA-IA's audit plans, and taking into account the results of previous audits. This ensures that the same CIS is not audited twice in the same year, although this could be done if necessary. In addition, the FIS internal controls are spread over different shoulders, ensuring that operative and security-related technical aspects are taken into account in the audited data processing operations.

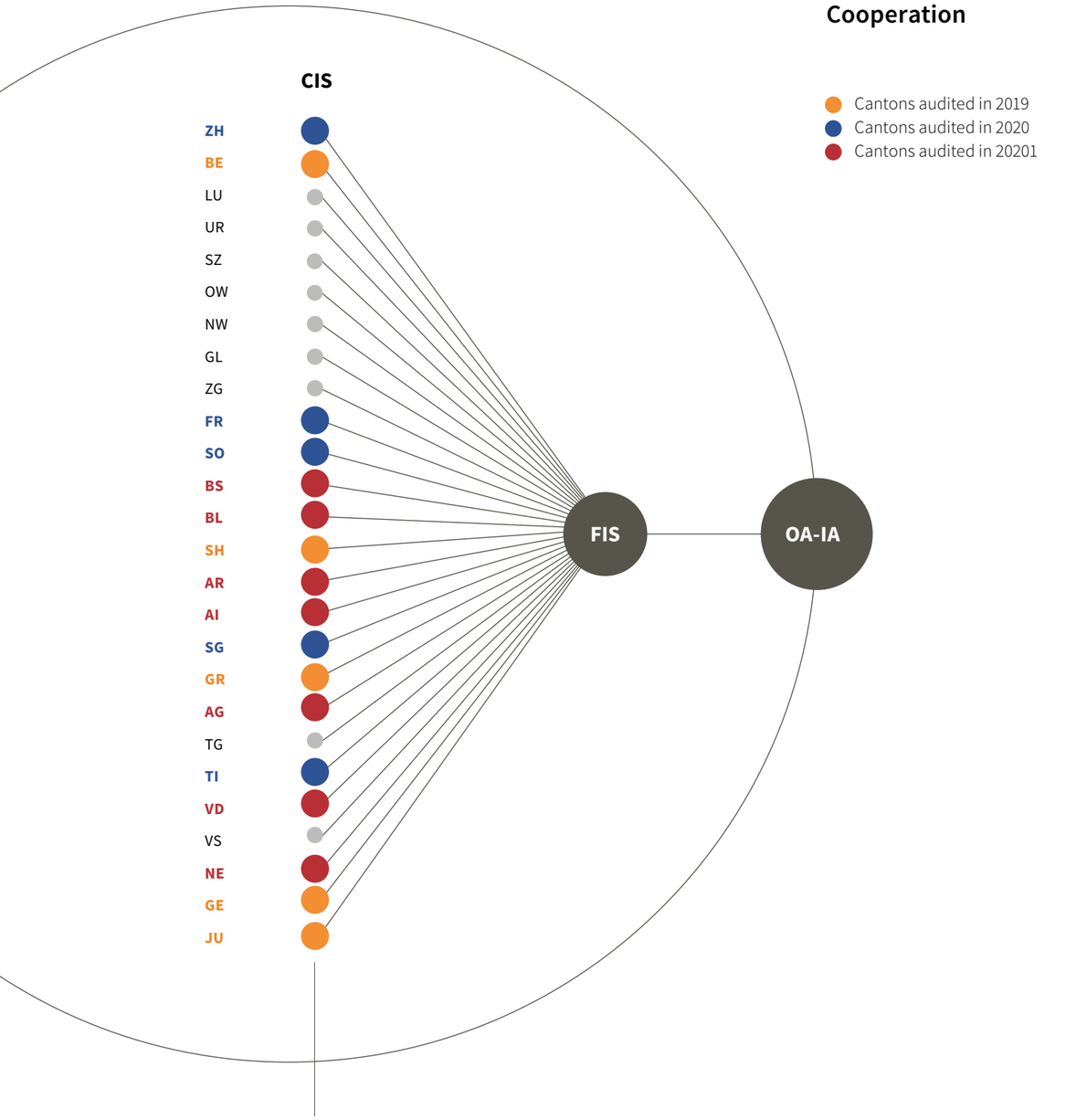
21-6 to 21-12: Audits of the CIS Basel-Stadt, Basel-Landschaft, Appenzell Ausserrhoden, Appenzell Innerrhoden, Aargau, Vaud and Neuchâtel (FIS/CIS)

In 2021, the OA-IA audited the intelligence activities of the CIS of the cantons of Aargau, Appenzell Ausserrhoden, Appenzell Innerrhoden, Basel-Landschaft, Basel-Stadt, Neuchâtel and Vaud, as well as their cooperation with the FIS. The OA-IA has thus audited a total of 17 CIS[27] since the start of its oversight duties. The remaining nine CIS will be audited over the next two years.

All CIS audits carried out in 2021 showed that the FIS and the CIS generally work well together in all areas of intelligence. However, with regard to implementation of joint operational procedures, there is a desire on both sides for better coordination. Differences of opinion between the FIS and individual CIS with respect to the annual performance review were settled in discussions to clarify the situation.

The CIS have good to very good intelligence knowledge and carry out the FIS's mandates on time, in accordance with the law and in a quality that is satisfactory to the FIS. The FIS provides the CIS with several intelligence applications and filing systems on the decentralised work platform (DezAP),[28] including a business management system (AV CIS) and a specialised

[24] Art. 70 para. 1 let. b and Art. 72 IntelSA
[25] Art. 5 para. 8 IntelSA
[26] Art. 72 IntelSA
[27] In 2020 the OA-IA audited the CIS of the cantons of St Gallen, Zurich, Ticino, Solothurn and Fribourg. In 2019, it audited the CIS of the cantons of Bern, Graubünden, Geneva, Jura and Schaffhausen.
[28] DezAP is part of the FIS's SiLAN secure network which provides access to the FIS's systems from a decentralised location. The term DezAP is also used for laptops to allow decentralised work. The CIS work platform (AP CIS) is a variation on the DezAP which the CIS are provided with.



Cooperation

- Cantons audited in 2019
- Cantons audited in 2020
- Cantons audited in 20201

150 FTEs

application (FA CIS) that allows the cantons to record objects[29] in a structured manner. The OA-IA found no data collections or personal data at the CIS for which there was no legal base for processing. However, some of the data in the specialised applications had not been recorded close to the time of the events or findings in question. As a result, some of this data had been stored in the specialised applications longer than the legally allowed five years. The reason for these incorrect data entries is assumed to be an earlier data migration in 2017/2018; the entries should disappear in the next two years as a result of the automatic deletion program. The OA-IA will follow this up in coordination with the QS FIS.

5.2.4 Information gathering

Information gathering is a core task of intelligence services. They can use various methods for this purpose. The OA-IA pays particularly close attention to methods that intrude most deeply into the privacy of the target person. In 2021 the OA-IA also carried out an extraordinary audit in the field of HUMINT. The FIS was notified of this audit in advance.

Die OA-IA conducted the following audits in this area in 2021:

- **21-13 Risk management for foreign operations(FIS)**
- **21-14 Operations (FIS)**
- **21-15 HUMINT (FIS)**
- 21-19 Extraordinary audit of HUMINT (FIS)

21-13 Risk management for foreign operations (FIS)

The FIS posts employees to carry out operations abroad. Target countries include those where the rule of law is only partially respected or not respected at all, or areas where security may be compromised. Sometimes the FIS is supported by third parties. Gathering information abroad is risky for the posted employees. The FIS must therefore ensure that these risks are not disproportionate to the expected benefit of the information they gather[30] and that its posted employees are protected.[31] Internal controls and processes are required to ensure these requirements are met. Appropriate and effective risk management is therefore important.

In this audit, the OA-IA focused in particular on operational missions from three areas of the FIS. In addition to conducting interviews and analysing documents, the OA-IA also compared FIS postings with those by the Federal Department of Foreign Affairs and the Federal Office of Police (fedpol).

The OA-IA found that risk management is in place for employees posted abroad, but that it is important to improve its expediency, largely to ensure the physical safety of posted personnel. It also concluded that the management of foreign missions should be centralised within the FIS, and processes should be standardised. The OA-IA can confirm that the involvement of third parties in high-risk missions abroad is lawful and clearly documented.

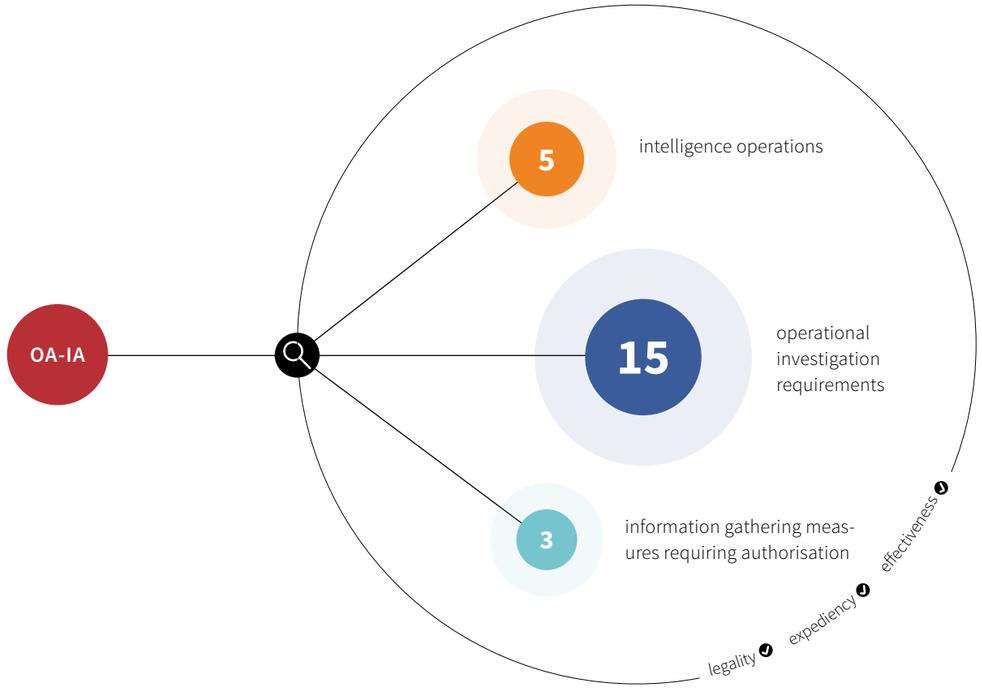
21-14 Operations (FIS)

The FIS conducts intelligence operations partly using information gathering measures requiring authorisation. Less time-critical and security-relevant operations involving information gathering measures that do not require authorisation are carried out as operational investigation requirements. The FIS reports annually to the Federal Council on operations; in the case of operational investigation requirements, the head of the DDPS is only informed of their content on an ad hoc basis and as required.

In an annually recurring audit, the OA-IA analysed five intelligence operations and fifteen operational investigation requirements for their expediency, effectiveness and compliance with the law. In addition, it examined three information gathering measures requiring authorisation to determine

[29] The objects most used by the FA CIS are people, events and means of communication.

[30] Art. 36 para. 3 IntelSA
[31] Art. 36 para. 7 IntelSA



whether their implementation complied with the decisions of the Federal Administrative Court. In previous years, these three areas were audited separately. However, since they contain many interfaces and interdependent aspects, the OA-IA decided to combine them into a single audit.

The audit comprised analysing documents and conducting interviews with the appropriate FIS specialists. Based on its findings from the audit, the OA-IA can confirm that the measures were generally carried out lawfully, expediently and effectively.

21-15 HUMINT (FIS)

Human sources remain one of the most important instruments in information gathering by intelligence services, despite highly developed methods for technical surveillance and access to a vast array of open source material. People with access to specific information are therefore of key importance to every intelligence service.

The public discovered in the Control Delegation's report 'Inspection following the arrest of a former FIS source in Germany' how the FIS uses human sources. In 2017, a former FIS source was arrested in Germany on suspicion of espionage. Following the arrest, the Control Delegation decided to examine the background to the case and the role of the FIS, the Federal Council and the Attorney General's Office. Implementing the recommendations of the report has had a lasting effect on the FIS's work with human sources.

Human intelligence often involves high personal risks for both FIS personnel and for the sources. This means the FIS has a special responsibility and obligation towards them, which it must take very seriously and which is given special weight in our oversight. Human intelligence officers (HUMINT officers), i.e. those who handle human intelligence sources, require specialised knowledge in their respective subject areas, comprehensive intelligence training and language skills. They must also have outstanding social skills and, above all, intercultural expertise and psychological sensitivity in order to the master the extraordinary challenges.

HUMINT officers need to understand what motivates and drives people, regardless of where they are from or what they do. Operational staff therefore receive special training in foreign languages, in the use of technology and in managing people. Moreover, life as a case officer entails many restrictions in private life.

The OA-IA examines the use of human intelligence at the FIS annually through random samples. The audits cover the whole spectrum of the management of human sources, including security risks, financial expenditure and the tangible impact of human intelligence. The OA-IA selects which cases to audit based on a risk assessment. It conducts interviews with the HUMINT officers, with the head of the HUMINT department and with employees from the Evaluation Division, who incorporate the information gained from human intelligence sources into their intelligence products.

"The OA-IA examines the use of human intelligence at the FIS annually through random samples. The audits cover the whole spectrum of the management of human sources."

The audits place special demands on confidentiality. For example, the names of the sources and HUMINT officers remain secret, even from the OA-IA, unless they are relevant to the audit. In concrete terms, this need-to-know principle means that only persons who require this personal data in order to perform their tasks have access to it.

The protection of sources is guaranteed by law.[32] The OA-IA must also fulfil these legal requirements in its audits. For reasons of national security, the OA-IA therefore cannot provide information about its audit results to the same extent as it does in other audit areas.

5.2.5 Resources

In order to ensure effective intelligence operations it is essential that resources are used expediently.

In 2021, the OA-IA did not plan or carry out any audits in this area.

5.2.6 Data processing and archiving

The information handled by intelligence services is extremely sensitive. The legal requirements for data processing and archiving are clear, but also complex. The OA-IA must therefore pay special attention to the lawfulness of information processing.

The OA-IA planned the following audits in this area in 2021:

- 21-16 Telecommunication Services (FIS)
- **21-17 Selected FIS Information System (Quattro P)**
- **21-18 Data Protection within the MIS**

Audit 21-16 'Telecommunication Services' was only launched in the final quarter of 2021. The findings from this audit were not yet available when this report was compiled.

21-17 Selected FIS Information System (Quattro P)

In 2020, the OA-IA decided to include the Quattro P information system in its 2021 audit plan. The reason for this is that the system stores and processes a large volume of data on the [travel] movements of certain categories of foreign nationals, and this personal data is also used for the FIS's facial recognition system, which the FIS has been using since 2020 but only for searching its own data. The number of Quattro P users is large; half of the FIS staff is now authorised to access the system. In its audit, the OA-IA examined the operation, use and content of the information system for its legality and expediency. A further part of the audit concerned the lawfulness of the facial recognition system used by the FIS.

As part of the audit, the auditors were granted access to the Quattro P, IASA FIS, SiLAN data storage and the facial recognition systems. This allowed the OA-IA to plan and carry out random sampling independently.

Lawfulness of data entry and processing in Quattro P

The Federal Council determines in a non-public list the categories of persons (travellers) that must be reported to the FIS without being requested to do so.[33] In doing so, it takes account of the threat situation at the time. Data on persons who travel within the Schengen area is not stored in the Quattro P database due to the absence of border controls.

[32] Art. 35 IntelSA

[33] Art. 55 para. 4 IntelSA; the list of countries is part of the list mentioned in Art. 20 para. 4 IntelSA (activities and data that must be reported without a request being made).

The following personal data is recorded in the Quattro P information system:[34]

- Surname, first name, date of birth, nationality;
- Identity document number, visa number, date of validity;
- Identity document photo;
- Place, date and description of the border control;
- Gender;
- Data from the identity document's chip;
- Data from the visa.

The data is supplied by the appropriate authority (border guard, police station), which also triages the information so that the FIS receives only data that is legally permitted. The data of children under 16 is not recorded.

After analysing the legal provisions and the information system's documentation, the OA-IA took random samples to examine whether the following data in Quattro P was in compliance with the law:

- data regarding the travel movements of nationals on the Federal Council list;
- data of children;
- compliance with five-year data retention period;[35]
- Quattro P entries and their recording in the IASA FIS system.

During the random sample audit, the OA-IA found cases of multiple entries of travel documents for individual travel movements. It therefore recommended that the FIS examine and take measures to reduce these cases. Otherwise, the OA-IA found the data in Quattro P to be in compliance with the legal provisions.

Expediency of data entry and processing in Quattro P

The term 'expediency' encompasses the suitability, necessity and appropriateness of a procedure or method, in this case the processing of data in the Quattro P system. Complicated and cumbersome data processing is prone to errors and may result in information relevant to the FIS fulfilling its tasks being available too late.

In view of the large volume of data supplied, the automated transmission of data from external sources seems to have proven a success. Only a small percentage of this data is post-processed manually. If the proportion of incorrectly supplied data increases, the FIS consults the authority supplying the data and appropriate measures are taken to improve its quality.

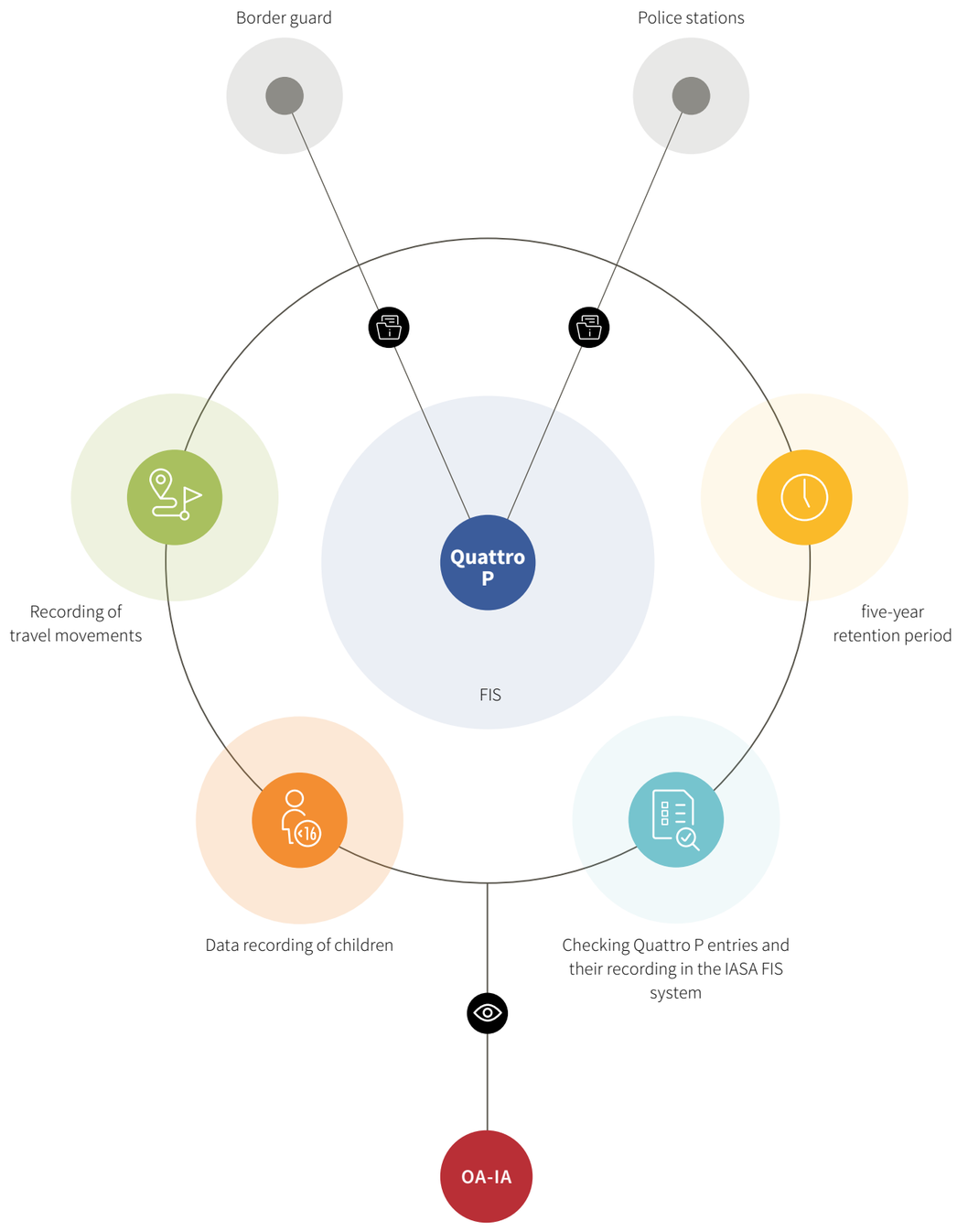
With regard to the random samples taken to verify the lawfulness of the data collected, the OA-IA found that in around 25% of the cases examined, the direction of travel was indicated as 'undefined'.[36] The OA-IA therefore recommended that the FIS and the oversight authorities examine what measures can be adopted to reduce this proportion.

Lawfulness and expediency of access management regarding Quattro P

For reasons of information security and data protection, access to Quattro P may only be granted to those FIS employees who need it to perform their tasks. Authorisations that are no longer required do not comply with the need-to-know principle. Inexpedient access management processes lead to a delay in updating access rights. These rights must be updated quickly if a member of staff changes function or leaves the service in order to avoid unauthorised access to data and the security vulnerabilities that may arise as a result.

[34] Annex 8 ISSO-FIS (Ordinance on the Federal Intelligence Service Information and Storage Systems)
[35] Art. 55 ISSO-FIS
[36] The following options are available: 'Entry', 'Departure' and 'Not defined'.

Quattro P



Based on the random samples carried out and an analysis of the relevant documents, the OA-IA recommended that access authorisations be regularly checked and deleted if no longer required.[37]

Lawfulness of the facial recognition system

Facial recognition systems can be used to identify people in photos, videos or in real time. The images available in data sets are analysed for the geometry of the captured faces. The characteristic analogue key features are transformed into a set of digital data – a facial print. This is as unique as the fingerprint. Such data is called biometric data.[38]

Facial recognition is a new search engine that is controversial from a data protection point of view. Since it is used at the FIS, the OA-IA decided to investigate the lawfulness of its use.

The OA-IA noted that at the beginning of the project the FIS conducted various inquiries to clarify the lawfulness of facial recognition. These inquiries were used to draw up processing regulations and to analyse the legal base for using facial recognition. The project subsequently developed further, but the FIS's legal service or quality assurance division did not check the lawfulness of these further developments.

The OA-IA is of the opinion that the data processed by the facial recognition system constitutes biometric data. According to the revised Federal Act on Data Protection Act (FADP),39 which is not yet in force, such data is classed as sensitive personal data. According to Article 47 paragraph 2 IntelSA, the Federal Council determines the catalogue of personal data that may be processed in each information system. This catalogue is listed in the Ordinance on the Federal Intelligence Service Information and Storage Systems (ISSO-FIS). However, the ordinance does not contain any provisions on processing biometric data in the information systems mentioned therein.

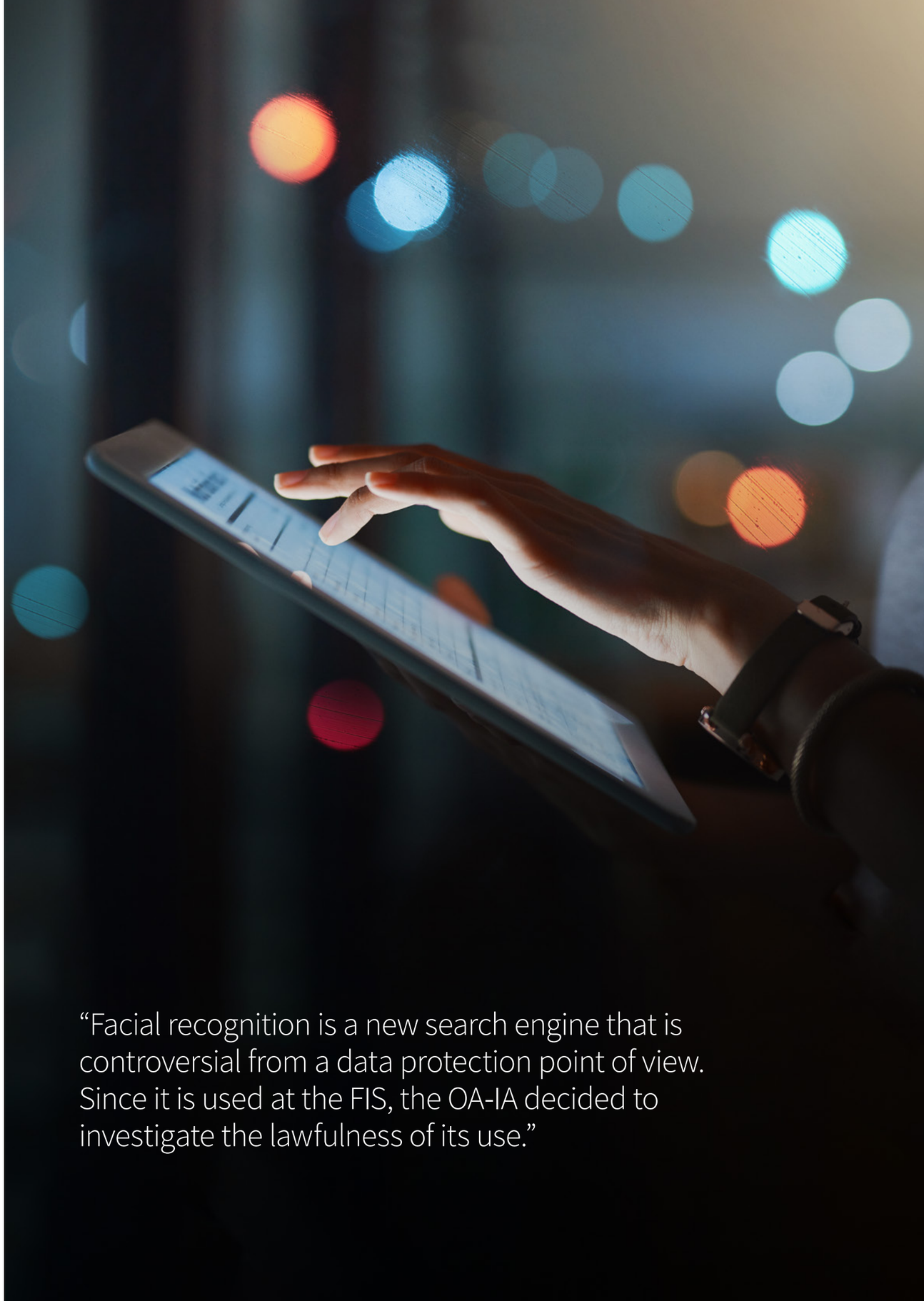
In addition, the facial recognition system can be used to create image profiles, which can be enriched with metadata. In the OA-IA's view, this leads to the creation of personality profiles. Based on these considerations, the OA-IA issued several recommendations, including the recommendation that the FIS include the Federal Data Protection and Information Commissioner in its further legal evaluations.

21-18 Data protection at the MIS

In audit 20-17, the OA-IA examined the information systems of the MIS that are relevant to intelligence activities. In the current reporting year, it examined in audit 21-18 the lawfulness of personal data processing in two systems. For this audit, the OA-IA conducted interviews, inspected documents and took random samples. Among the various information systems, sub-systems and special applications, the OA-IA focused on the information systems operated by and under the responsibility of the MIS: the Information System for Military Intelligence (IK MIS) – its main working instrument – and the information system for secure information sharing with foreign states, known as BICES.[40] In our view, these systems pose the greatest data protection risk on account of the volume, type and recipients of the data as well as the potential impact of violations against personality rights for those concerned.

The OA-IA noted that the MIS processes personal data as part of its legal duties and that the processing of sensitive personal data or the creation of personality profiles may also

[37] Art. 5 para. 4 ISSO-FIS
[38] Source: www.kaspersky.de/resource-center/definitions/what-is-facial-recognition, last viewed on 22.11.2021
[39] SR 235.1
[40] Battlefield Information Collection and Exploitation System, the international communication network of NATO



“In the year under review, the OA-IA noted a marked increase in informal information indicating the dissatisfaction of FIS staff.”

be necessary as part of these duties. However, the OA-IA did not come across any such instances during its audit of random samples. The OA-IA found that although personal data is present in certain MIS reports, this personal data is not the focus of MIS interest. The MIS focuses on gathering and evaluating information that is important for the Armed Forces (in particular for the defence of Switzerland) and for promoting peace and providing support services abroad. The information it gathers largely concerns foreign countries and not people in Switzerland; these people are not recorded in the MIS's information systems in a structured manner. Personal data collected in the context of providing support services in Switzerland (for example at World Economic Forum meetings) is forwarded to the appropriate Swiss authorities and may not be used in connection with military intelligence activities.

Where personal data is processed, it concerns the names of people from politics, of foreign leaders and of activists from armed networks or organisations. This information enables the MIS to monitor and assess military strategic developments and armed forces. The focus is on specific countries, military threats, armed conflicts and regions abroad where the Swiss Armed Forces are deployed.

In each case examined by the OA-IA in the random sample audit, a link to the activities of the MIS was found. The OA-IA was also explained users' access rights and the processes for archiving and deleting documents. It noted that access is limited to those members of staff who require it for their tasks. The reports in the information systems examined are sent to the Swiss Federal Archives and not retained over the legal deadline. The information systems used by the MIS are well documented and are not connected via common interfaces that would allow for automatic data exchange. This minimises the risk of misuse.

During its audit, the OA-IA did not identify any issues that led it to doubt the lawfulness of personal data processing by the MIS at any stage. Nor did the OA-IA discover any misuse or disproportionate use of the personal data collected according to the law or to data protection legislation.

The OA-IA further noted that the MIS relies on specific provisions for transmitting personal data abroad. The reports it transmits abroad generally comprise situation analyses of a military, political or military policy nature. While it cannot be ruled out that personal data may occasionally appear in MIS reports, there is no exchange of information on specific individuals. Furthermore, MIS reports are only transmitted to the services of countries that share Western values and have data protection laws.

5.3 Acceptance

In the course of their work, the OA-IA auditors were received by all audited entities in a constructive and professional manner. They were given access to the documents and information systems needed to carry out their audits. The interviewees were available to the auditors. The interviews could be planned and conducted in a timely manner despite the COVID restrictions. Additional questions were answered as quickly as possible.

In the year under review, the OA-IA noted a marked increase in informal information indicating the dissatisfaction of FIS staff. The OA-IA analysed this information where necessary and possible, and either incorporated it into its audit procedures or dealt with it individually. The head of the DDPS was informed in writing about these developments on 13 July and 22 October 2021. This is an ongoing issue that will continue to draw our attention also in the future.

5.4 Controlling of recommendations

Controlling the implementation of recommendations is not explicitly regulated by the IntelSA. In agreement with the DDPS and the audited services, it was agreed that the latter would inform the DDPS in writing of progress made in implementing the OA-IA recommendations and that the OA-IA would receive a copy of those progress updates. For 66 recommendations a notification was made in 2021. By the end of 2021, no further recommendations were pending at the MIS or EOC. In addition, a meeting was held in the middle of the year with all the audited services and in the presence of a DDPS advisor to the DDPS head to take stock of the current state of implementation.

Monitoring implementation of the recommendations – An example

With the entry into force of the IntelSA, the FIS was given a legal base for posting its own personnel to Swiss representations abroad in order to promote international contacts.[41] The FIS makes use of this possibility through intelligence liaison officers. Therefore, in 2019, the OA-IA audited the management of intelligence data between the defence attaché network and the FIS.

The defence attaché network assists in implementing Switzerland's foreign and security policy interests. Although the attachés are members of the Swiss Armed Forces, the FIS is primarily responsible for their posting and for managing their intelligence activities.

As a result of the 2019 audit, the OA-IA recommended that the FIS draws up a strategic plan to better define the posting of intelligence liaison officers and their interface with the defence attachés. The purpose of this was to improve expediency and effectiveness in this area of intelligence.

In 2021, the OA-IA conducted audit 21-1 ‘Deployment of FIS Employees to Swiss Representations abroad’. A key element of the audit was to review implementation of the recommendation to compile a strategic plan for posting intelligence liaison officers abroad. Recommendations are recorded in a monitoring system at the OA-IA and checked against an implementation report from the FIS. The OA-IA then decides whether the implementation measures are sufficient or whether a more- in-depth review is necessary. If a more in-depth review is necessary, it is either integrated into an audit that has already been planned or, as in the case described above, a separate audit is carried out.

[41] Art. 12 para. 2 IntelSA

6. Insights from inside

In this section, the OA-IA reports on its internal affairs.

6.1 Personnel and continuing training

The OA-IA still has 10 employees (9.1 full-time equivalents). Two auditors and the office manager decided to take up a new challenge and left the OA-IA at the end of the year. Their successors had been found by the end of November, and the OA-IA will once again be fully staffed during the first six months of 2022.

Many employees made use of the training opportunities available to them in 2021. Staff members took demanding qualifications such as Masters degrees and CASs[42] in technical fields and management. The placement with Comité R in Belgium, already planned back in 2020, had to be postponed once again.

The system of working from home, as dictated by the COVID-19 restrictions, generally worked well. However, challenges are faced when classified information has to be processed. Over the weeks and months spent working from home, the lack of direct contact and discussion between colleagues began to take its toll; technical aids cannot compensate for this. The induction of new employees does not work well in such an environment and may well prolong the time necessary before they can conduct audits.

6.2 IntelSA revision

The draft revised IntelSA underwent consultation in 2021. The OA-IA was able to have an influence on the text, particularly in Chapter 6, which directly concerns the OA-IA. The DDPS has the lead in the revision project.

6.3 Federal Act on Freedom of Information in the Administration (Freedom of Information Act, FoIA)

The OA-IA did not receive any applications for access to official documents in the year under review.

6.4 Visits

The head of the DDPS visited the OA-IA premises in September to become acquainted with its work.

In January the OA-IA also invited the Control Delegation (CDel) to visit its premises in order to gain an insight into the OA-IA's practical work. The CDel did not take up the invitation.

6.5 Jurisdiction

The OA-IA monitors court decisions at national and international level. In the year under review, rulings by the European Court of Human Rights were analysed internally and discussed by the team. The OA-IA also received important inputs on the administration of justice at European level at the European Oversight Conference in Rome.

[42] Certificate of Advanced Studies, part-time post-Master's academic certificate

7. Coordination

The OA-IA coordinates its activities with parliamentary oversight activities with those of other federal and cantonal oversight bodies.[43] However, in 2021 the pandemic and the measures and travel restrictions it involved continued to impact this coordination.

7.1 National contacts

Conference with cantonal oversight bodies

On 18 August 2021 the OA-IA held its second conference with the cantonal oversight bodies (COB) in the military barracks in Bern. Fifteen COB, FIS members and the two CIS heads took part. The conference provided opportunities for learning, networking and discussion.

The conference was launched by members of two COBs (Solothurn and Fribourg), who spoke about their results, the challenges they face and their expectations. Two FIS members then presented their perspective, in particular with regard to quality and security checks and administration in general. The heads of the Basel-Stadt and Fribourg CIS also spoke at the conference, explaining how oversight impacts their work. In the final presentation, the head of the OA-IA talked about his organisation's activities since the last conference, which took place in 2018. In the podium discussion held in the afternoon, the four participants examined core issues and ideas about how intelligence oversight may go forward.

Conference outcomes:

The cantonal oversight bodies focus primarily on the legality of the CIS' activities. It is a constant challenge to use human sources effectively, maintain oversight lists, maintain an overview of the threat situation and ensure sufficient distance from the work of the police services. At the same time, transparency, dialogue and understanding are key elements in creating trust.

The FIS underlines the importance of coordinating and exchanging with the CIS. It notes that considerable progress has been made since the IntelSA came into force in September 2017. However, there are still different approaches to data processing and cooperation among the CIS. The FIS urges them to report irregularities at any level as swiftly as possible, stating that "Together we are strong, and together we can ensure security in Switzerland."

In the eyes of the CIS, de-mystifying intelligence activities should be the principal objective of oversight. Discussions with the oversight authorities are generally very constructive. They allow the intelligence services to report any needs they may have, increase transparency and trust, and create potential for development and improvements. However, it was noted that the CIS must undergo a vast number of audits by cantonal and national oversight bodies (as much as one audit a month in the case of one particular CIS), and that better planning of the audits among the various authorities would be desirable. The point was also raised that there are considerable legal obstacles in conducting intelligence-gathering activities requiring authorisation. As a result, intelligence information is increasingly being gathered from human sources.

For the OA-IA, the audits conducted since the IntelSA came into force, cooperation between the various oversight actors, information flows and the CIS' involvement are clearly positive points. However, it sees room for improvement in data processing, the use of resources and the use of technical means. The declared aim should undoubtedly be to increase the status of intelligence activities and to build trust.

[43] Art. 78 para. 2 IntelSA.

Having previously been postponed because of the uncertainty of the COVID-19 pandemic, the conference in 2021 was a great success. It will be held again in 2023.

Federal Administrative Court (FAC)

On 10 September 2021 the OA-IA met members of the FAC to discuss a variety of topics, including information gathering measures requiring authorisation, recent court rulings and the revision of the IntelSA.

Swiss Federal Audit Office (SFAO)

On 21 May 2021, the OA-IA management met with two members of the SFAO to discuss and coordinate a number of issues, including possible audit topics.

Control Delegation (CDel)

The OA-IA was invited to one hearing only, on 20 January 2021, at which the management and an employee reported on audit 20-13 Operational clarification needs. We consider the CDel's reporting on the OA-IA to be one-sided and unbalanced. The OA-IA sent a four-page letter commenting on the CDel's draft annual report. The majority of the requested changes were not considered and no feedback was given. We do not find this kind of reporting to be constructive, either with regard to the subject matter or in terms of the impression made. The OA-IA hopes that it will soon be possible for the authorities concerned to discuss the oversight of intelligence activities in a reasonable fashion.

DDPS Internal Audit Service (DDPS IAS)

In a telephone conversation held on 22 January 2021, the OA-IA management and DDPS IAS management discussed how the IAS could benefit from information held by the OA-IA and how oversight can also generate added value for the services. They also discussed introducing a kind of peer-review system in the OA-IA, whereby the processes of one oversight body could be examined for expediency by another body.

Basel-Stadt cantonal services oversight body

The head of the OA-IA and two audit managers met representatives of the Basel-Stadt cantonal services oversight body on 15 July 2021 to discuss a variety of topics, including their annual reports, auditing in the field of violent right-wing extremism, the impact of the Federal Act on Police Counterterrorism Measures, oversight methods and audit report 21-6 Audit of CIS Basel Stadt.

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

The revision of the IntelSA should provide a legal basis for the merger between the ICA and the OA-IA, which was already discussed when the IntelSA was first drawn up. To this end, the ICA president and the head of the OA-IA agreed that the OA-IA would attend the ICA's regular audit meetings; an OA-IA representative attended the ICA meetings on 26 June, 17 September, 22 October and 18 November 2021.

The aim was to gain an overview of the audit activities and thus build up the technical and intelligence expertise necessary for the OA-IA to take over the ICA's activities. The OA-IA refrained from playing an active role in the ICA's audit process, as it lacked the authority to do so. The ICA reports annually to the CDel, and the OA-IA receives the report in each case for information purposes.

In addition, the OA-IA took part in the K-workshop, to which the ICA regularly invites representatives of the FIS, EOC, FAC and OA-IA to exchange information on cable communications intelligence. This year, topics ranged from the expansion of technical infrastructure, the particular challenge of controlling radio and cable communications intelligence and the legal hurdles when extending orders for this kind of intelligence.

OA-IA/FIS management retreat

In the Koller report of March 2013 on the tasks, organisation and performance of DDPS intelligence oversight, a recommendation was made to hold an annual retreat for the oversight body and the FIS as the start of a long-term strategy development and to identify (large-scale) political risks.

The FIS and the OA-IA now have four years of shared experience, yet this recommendation is still pertinent even in the changed environment of today and is supported by the FIS. On 2 November 2021, the extended FIS management came together with the OA-IA for the retreat, which was also attended by the intelligence advisor to the head of the DDPS. The aim of this first event was to promote mutual understanding and acceptance and to decide how to proceed. It was agreed that the retreat was useful and that it would be a good idea to hold a further one, to be attended by the new OA-IA head.

The OA-IA management held discussions with the following people at least once in 2021:

- Head of the DDPS
- DDPS Secretary General
- FIS director/deputy director
- Head of the MIS
- Head of the EOC
- FDPIC staff

The meeting with advisors from the FDFA, FDJP and DDPS (attendance at the Federal Council Security Committee meeting) had to be postponed and did not take place in 2021.

Enquiries from Citizens

In 2021 the OA-IA received and dealt with 11 enquiries from citizens.

7.2 International contacts

The OA-IA can only oversee Switzerland's intelligence activities within the country's borders. There is currently no legal basis for exchanging information with partner authorities. The OA-IA can, however, exchange information on oversight methods, processes and experiences.

Virtual meeting, 20 September 2021: Intelligence Oversight Working Group (IOWG)

Before the pandemic, the IOWG met twice a year. As its last face-to-face meeting was in January 2020, shortly before the introduction of COVID-19 restrictions, this virtual meeting was held to maintain contact and to discuss how the working group will organise itself going forward.

Rome, 7 and 8 October 2021: European Oversight Conference

Italy's General Prosecution Office organised a meeting between several countries to discuss various national and international court rulings and their impact on the respective intelligence services and associated oversight bodies. Besides the representatives of the Italian oversight bodies, delegates from Austria, Belgium, Bulgaria, Denmark, France, Germany, Greece, Luxembourg, the Netherlands, Norway, Portugal, Switzerland and the United Kingdom also attended.

8. A view from outside (carte blanche)

The annual report also includes an external perspective on the OA-IA's activities. In keeping with the theme of this report's focus on information systems, Adrian Lobsiger presents his personal view of matters.

Opportunities and risks of digital transformation

The Secret Files Scandal in 1989 caused an abrupt loss of confidence among the Swiss public in the national security service. Once the scandal concerning mass surveillance by the federal police (then known as 'BUPO') had been investigated and processed, politicians demanded that the many different tasks conducted by this security service be disentangled. In the face of a political initiative to completely abolish the national security service, which was only rudimentarily regulated at the time, the Federal Council and Parliament launched a process to introduce some controls. A referendum held in 1998 permitted the continuation of national security activities and formally regulated them in law. In a second referendum in 2016, the current IntelSA was adopted, authorising the FIS to acquire personal data not only by (mainly) covert but also by coercive means. The ban on the use of coercive means having been removed, Parliament set up an independent oversight authority exclusively for the FIS.

Even though opinions about intelligence surveillance still differ, its critics must concede that, since the introduction of the IntelSA, data processing by national security services is based on a law that is clear and sufficiently specific. In contrast, much still needs to be done before we have clear legislation on the equally highly sensitive processing of personal data by other federal security authorities. For example, data processing by fedpol and the Swiss Border Guard is based on a large and growing number of special provisions scattered throughout various pieces of legislation. Furthermore, the federal security authorities have launched a number of wide-ranging projects for digital transformation which make it even more difficult for the general public to understand how the law handles the processing of personal data. Because these projects can have far-reaching consequences for the processing of personal data, the federal data protection oversight authority is working to ensure that processes are fully recorded and analysed at the planning stage in data protection impact assessments.

In its strategy for digital transformation in the administration, the Federal Council has called for traditional forms of living and doing business together to be questioned and rethought, and for an expansion of digital skills that enable networking and data-sharing between all stakeholders. Words create images, and so some promoters of digital transformation see in their mind's eye a cloud from which police forces, border guards and intelligence services draw information for the benefit of all law-abiding people who have nothing to hide.

The antithesis of this vision is the much frowned-upon keeping of data in 'silos', seen by digital transformation proponents as the relic of an outdated way of thinking that – as some would claim – is typical of a system of data protection that favours perpetrators instead of protecting citizens. The fact that each canton has a police force that processes the personal data accruing there on its own responsibility and usually only shares it with other security authorities upon request leads these visionaries to shake their heads, as does the fact that the federal

Adrian Lobsiger (*1959)
After his studies in Bern and Basel, Adrian Lobsiger, born on 27 December 1959, obtained a master's degree in European law from the University of Exeter (GB). In 1992, he began his career in the field of international private law at the Federal Office of Justice. In 1995, he joined the Federal Office of Police (fedpol), where he became deputy director.

Adrian Lobsiger was elected by the Federal Council in November 2015 and confirmed by Parliament in March 2016. He has been in office since June 2016. At its meeting on 10 April 2019, the Federal Council confirmed the re-election of Adrian Lobsiger as Federal Data Protection and Information Commissioner (FDPIC) for a second term of office until the end of 2023.

government distributes its police power among three federal offices. As sworn opponents of data silos, they feel aggrieved by this state of affairs, and in order to bring about long-overdue change, are pushing for all security authorities to be linked as far as technically feasible.

If one disregards the historical events that led the writers of the Constitution to organise communities federally and to divide centralised power, it is difficult to understand the rationality of complex data flows among the state security authorities. However, if the historical context is taken into account, it can be seen that Switzerland's internal security system has emerged from a sequence of decisions made by its political institutions and shaped directly by the public in popular votes and referendums. This is what happened, for example, in 1978 with the successful referendum against the creation of a federal security police authority; to this day, this veto against a central security authority at federal level has not been revoked.

A new way of thinking that sees the digital availability of personal data as the measure of all things and ignores political concepts to limit state power takes us backwards, not forward. It takes us back to the police state, which was abolished when absolutist aristocracies were overcome in the bourgeois revolutions of the 18th and 19th centuries. When the omnipotent power structures of the ancien régime were dismantled and replaced by specialised offices, this greatly helped to transform the police state into a public service and to turn subjects into self-confident citizens who, in return for paying taxes, could demand professional and discreet services from these offices.

Legal procedures govern the way these specialised offices share the data they hold on citizens, and this forms part of the professionalism demanded of them. That the Federal Administration now prepares factual data in a machine-readable form and makes it usable across departments and offices is also an expression of this professionalism. It also records master data and personal attributes according to the so-called once-only principle and manages them using uniform identifiers such as the AHV number. Data protection does not stand in the way of digitalisation processes, which make public services more efficient, especially since these processes can also help to improve data quality.

Yet should anyone try to create a kind of cloud of non-transparent networks, from which the security authorities, tax investigators and other agencies of the ‘interventionist administration’ could extract all the data that accumulates when members of the public interact with the public authorities, this would set them on a collision course with data protection standards. Such a data grab would soon stink to high heaven and poison public trust in the state's role as a public service and guarantor of the rule of law. To prevent this, the Federal Data Protection and Information Commissioner requires those responsible for digital transformation projects to declare in the data protection impact assessments the scope and intensity of future data processing and to state the entities authorised to access the data and make a comparison with the status quo. Any planned extension or intensification of existing personal data processing activities must be justified.

The federal offices sometimes argue that digital transformation projects must be planned in an ‘agile’ manner because of the rapid pace of technical progress. They claim that it is therefore not possible to define future data processing definitively, or to compare it with the status quo. Such arguments are untenable; they are tantamount to giving the Federal Administration blanket authorisation, since neither the political bodies that are responsible for official interventions in the private sphere of the general public nor the general public themselves can assess what ‘agile’ risks might be. The Federal Data Protection and Information Commissioner repeatedly sees it as his duty to ensure that data protection impact assessments are detailed and extensive before their results are included in the dispatches in which the Federal Council proposes to Parliament amendments to security legislation.

In view of the challenges described above, the Commissioner considers himself fortunate that his work in the intelligence field is complemented in a purposeful manner by the independent FIS oversight authority.

9. Key figures as of 31 December 2021

Stuff

1 January 2021	**10**
31 December 2021	**9**
Resignations	**4**

Audits

Planned audits	**18 (18)**
Unannounced audits	**0 (1)**
Audits conducted	**18 (17)**

Interviews 2021

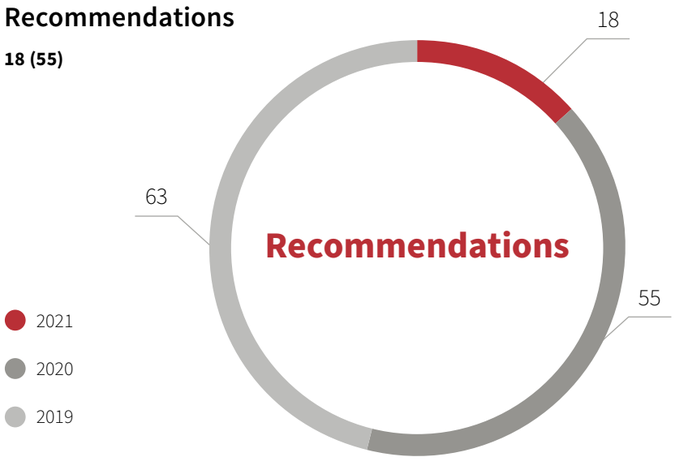
90 (102)

Budgeted workforce

10

Recommendations

18 (55)



10. Appendix

10.1 2021 Audit Plan

No.	Name of audit	Service audited
Strategy and Planning		
21-1	Deployment of FIS[1] employees in Swiss representations abroad	FIS
Organisation		
21-2	Critical infrastructure protection / cyber defense	FIS / EOC[2]
21-3	FIS security	FIS
21-4	Violent right-wing extremism	FIS
Cooperation		
21-5	FIS quality assurance within the Cantonal Intelligence Services (CIS)	FIS
21-6	Audit of CIS Basel-Stadt	FIS / CIS
21-7	Audit of CIS Basel-Landschaft	FIS / CIS
21-8	Audit of CIS Appenzell Ausserrhoden	FIS / CIS
21-9	Audit of CIS Appenzell Innerrhoden	FIS / CIS
21-10	Audit of CIS Aargau	FIS / CIS
21-11	Audit of CIS Waadt	FIS / CIS
21-12	Audit of CIS Neuenburg	FIS / CIS
Information gathering		
21-13	Risk management for foreign operations	FIS
21-14	Operations	FIS
21-15	HUMINT[3]	FIS
Resources		
	No audit planned	
Data Processing / Data Storage		
21-16	Telecommunication Services	FIS
21-17	Selected FIS Information System (Quattro P[4])	FIS
21-18	Data protection within the MIS[5]	MIS

1 Federal Intelligence Service
2 Electronic Operations Center
3 Human Intelligence
4 Art. 55 of the Federal Act on the Intelligence Service (Intelligence Service Act, IntelSA, SR 121)
5 Military Intelligence Service

10.2 List of abbreviations

AHV number
Old-age and survivors' insurance number

Art.
Article

AV CIS
Business management system used by the CIS

BBl
Federal Gazette

BICES
Battlefield Information Collection and Exploitation System (the international communication network of NATO)

BURAUT
Data storage system of the FIS

BUPO
Federal Police (Bundespolizei)

CAS
Certificate of Advanced Studies

CCPCS
Conference of Cantonal Police Commanders of Switzerland

CDel
Control Delegation

CIS
Cantonal intelligence service

COB
Cantonal oversight body

CNO
Cyber Network Operations

CTI
Cyber Threat Intelligence unit at the EOC

CYBER FIS
Cyber division at the FIS

DDPS IAS
Internal Audit Service of the Federal Department of Defence, Civil Protection and Sport

DDPS
Federal Department of Defence, Civil Protection and Sport

DezAP
Decentralised work platform

EOC
Electronic Operations Centre

FAC
Federal Administrative Court

FA CIS
Specialised application used by the CIS

FADP
Federal Act on Data Protection

FDJP
Federal Department of Justice and Police

FDPIC
Federal Data Protection and Information Commissioner

fedpol
Federal Office of Police

FIS
Federal Intelligence Service

FISA
FIS Evaluation Division

FoIA
Freedom of Information Act

GEVER FIS
Business management system of the FIS

HUMINT
Human intelligence

IASA
Integral analysis system of the FIS

ICA
Independent Control Authority for Radio and Cable Communications Intelligence

IK MIS
Information system for military intelligence

IntelSA
Intelligence Service Act

IOWG
Intelligence Oversight Working Group

ISSO-FIS
Ordinance on the Federal Intelligence Service Information and Storage Systems

JCTAC
Joint Cyber Technical Analysis Center

let.
Letter

MELANI OIC
Operations Information Centre at the Reporting and Analysis Centre for Information Assurance

MIS
Military Intelligence Service

No
Number

OA-IA
Independent Oversight Authority for Intelligence Activities

para.
Paragraph

QS FIS
Quality assurance office at the FIS

Quattro P
Information system used by the FIS to log special categories of foreigners entering and leaving Switzerland

SFA
Swiss Federal Archives

SFAO
Swiss Federal Audit Office

SiLAN
Secure network of the FIS

SR
Classified Compilation of Swiss Legislation

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