Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Independent Oversight Authority for Intelligence Activities

Annual Report 2019
of the Independent Oversight Authority for Intelligence Activities OA-IA

1. Summary

The OA-IA had initially planned to carry out a total of 21 audits for 2019.[1] Audits 19-13 (Hiring, support and departure process), 19-15 [Operation, content and use of the information systems GEVER FIS, BURAUT data storage and SiLAN data storage (temporary evaluations)] and 19-16 (Classification of information) related to various services or systems and were therefore broken down into two to three separate audit reports. The OA-IA was unable to carry out two of the originally planned audits, 19-17 (MIS information system landscape) and 19-21 [Access to/from third-party information systems (federal level, cantonal level, foreign agencies, law enforcement)] due to prioritisation of other activities. Audit 19-19 was started shortly before the end of December 2019 and therefore no information is provided about it in this Annual Report.

2019 was the first year that the OA-IA began auditing cooperation between the Federal Intelligence Service (FIS) and cantonal intelligence services (CIS). Five CIS were chosen: Geneva, Jura, Bern, Graubünden and Schaffhausen. In nearly all cantons, CIS are part of the cantonal police force and are receive most of their funding from the Federal Administration. In 2019, CIS positions accounted for roughly 124 full-time equivalents (FTEs). For the purpose of evaluation, the OA-IA developed a standardised audit format and made various recommendations of an organisational nature.

With regard to information-gathering measures requiring authorisation (IGMRAs) and operations, the OA-IA carried out five audits and four audits relating to data processing and file storage.

The number of people subjected to IGMRAs is miniscule considering the total size of the population[2]. The OA-IA feels that the FIS uses its most invasive tool proportionately. With IGMRAs, the FIS encroaches deeply on the fundamental rights the person affected and therefore the FIS's tendency to show restraint when using this tool is expedient. The OA-IA will continue to closely monitor future developments in this area.

The OA-IA mainly observed that there was room for improvement in the area of data processing. The FIS must be in a position to clearly explain why and what type of information about specific individuals is saved and used in its databases. The FIS can also set higher standards when it comes to structuring and systematically following data deletion procedures. The considerations required for this are complex, especially from a technical standpoint. It is also important to bear in mind that intelligence services are expected to produce forecasts. A basic underlying principle of intelligence is to think of the impossible and then construct scenarios on this basis. It is often unclear in the present what fundamental data will be needed in the future to construct these scenarios.

Audited bodies are required by law to be transparent with supervisory bodies and the latter are granted access and the right to view documents, processes and premises that are not only inaccessible to the general public but also in some cases intentionally hidden from public view. The audited bodies provided the OA-IA with this access and insight in all cases and in all situations.

The OA-IA made numerous recommendations for improvement of organisational aspects, structures and processes at the FIS. According to Article 78 paragraph 7 of the Intelligence Service Act (IntelSA)[3] the Federal Department of Defence, Civil Protection and Sport (DDPS) is responsible for ensuring implementation of OA-IA recommendations. It therefore requires the FIS, the MIS and the Electronic Operations Center (EOC) to implement OA-IA recommendations. The DDPS generally also requires that audited bodies implement OA-IA advisory notices, which technically are not legally binding. In 2019, the OA-IA formulated 63 recommendations and 40 advisory notices. Implementation of OA-IA recommendations can further reduce existing risks and improve efficiency, which the OA-IA feels is particularly important given current plans to hire additional FIS personnel.

Both of Switzerland's military intelligence services, the MIS and EOC, have more narrowly defined responsibilities. Both the MIS and EOC are dependent on the FIS to a certain extent. Both intelligence services seek to position themselves in relation to the FIS, optimally fill their respective niches and leverage and improve synergies.

In addition to its auditing activities, the OA-IA also took the time to look beyond the national and international context, to further refine its sense of its core mission, to share knowledge and to pursue greater cooperation with our partners and addressees.

The present Annual Report[4] was submitted to the DDPS and to the Controll Delegation of both chambers of Parliament for consultation from 13 to 23 January 2020. All feedback provided to us in relation to any formal or substantive errors found in the Annual Report or any overriding interests that might be compromised by publication of certain parts of the Annual Report has been taken into account.

[1] The audit plans have been posted on www.ab-nd.admin.ch.
[2] In 2018, a total of 28 persons were investigated in this manner, see also the FIS Annual Report entitled, "Switzerland's Security 2018"

[3] CC 121

[4] Excl. chapters 3 and 8

2. Table of Contents

3. Personal

Thomas Fritschi, Head of OA-IA

"Arrests of Swiss citizens for terrorist activities; emerging right-wing extremism; obsessive monitoring of large swathes of the Swiss population by the FIS and corresponding secret files on Swiss citizens; mass surveillance; cyber attacks; post-conflict return of jihadists and terrorist suspects; Russian spies and peace-time intelligence activities. These are some of the intelligence-related topics covered by the media over the previous year. Do you still remember them?

Depending on your own level of concern and interest, you may still vaguely recall some of the news reports. After the press conference on last year's annual report, one journalist was somewhat disappointed that the Independent Oversight Authority for Intelligence Activities (OA-IA) had not presented any real intelligence scandals and obviosously sees this an an indicator for our work. On the contrary, it seems to me that the fewer scandals, the better the oversight

"Transparency is the common theme running through this entire report."

Thomas Fritschi

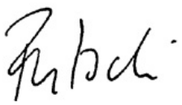
In 2019, we conducted 19 on-site audits of the intelligence services. We held around 119 interviews with employees and were given unfettered access to FIS databases. All in all, we were provided with a clear insight into Swiss intelligence activities. We gladly include part of this transparency in this report. This Annual Report gives us the chance to clarify the role of intelligence activities and for this reason transparency is a common theme running through this entire report.

Martin Stoll will present this year's view from outside. As a Sonntagszeitung news correspondent specialised in federal government-related matters, he is also the initiator of the Öffentlichkeitsgesetz.ch website, which is run by an independent association. The aim is to establish the Freedom of Information Act as a key legislative instrument for members of the press in Switzerland. He shares his viewpoint on the subject from page 33.

November 2019 marks the thirtieth anniversary of the Secret Files scandal that brought the Swiss government's mass surveillance activities to public attention. I was twenty years old at the time, the Berlin Wall had just fallen, and it would be many years before I would have an e-mail address or even a smartphone. From an intelligence standpoint, the threat situation had changed tremendously, as had the structure and legal basis of the intelligence services. Nowadays technology has placed our data processing capabilities on a whole new level. The digitalisation revolution presents society with some enormous challenges and the intelligence services now need to trawl through huge amounts of data to find key information enabling early detection of threats. And they need to be faster and more reliable than the media. At the same time, they must avoid gathering and hoarding inaccurate or excessive quantities of information. This is a very challenging task for the intelligence services.

We supervised the fulfilment of these tasks and found that many activites were carried out correctly, but also that mistakes had been made. In individual cases, too much data had been kept for too long or careless reports had been drafted. We are also of the opinion that the effectiveness of the intelligence services could be further enhanced by making organisational adjustments and optimising processes.

Through our work, we want to help eliminate or at least mitigate the risks associated with intelligence activities, while at the same time respecting and upholding the fundamental rights of people living in Switzerland. I hope you will enjoy reading this report."



Thomas Fritschi, Head of OA-IA

4. Transparency and secrecy

In order to pursue our vision of “We strenghten trust”, it is extremely important that the OA-IA be able to report openly to the head of the DDPS, to the intelligence services and to the Swiss population. The latter is a challenging task and we shall go over the various reasons for this in the following section.

4.1 How much transparency is the general public entitled to?

Explaining the work of intelligence activities is a balancing act for us. On the one hand, there are certain key intelligence principles that apply such as a “need to know” and it is also important to maintain a large degree of secrecy and discretion. On the other hand, our aim is to encourage the population to show understanding for intelligence activities. However, the Swiss population tends to feel sceptical when information is withheld and when government action – in this case intelligence – does not make sense.

The remit of the Swiss intelligence services is to prevent sensitive information from falling into the hands of those who might pose a security risk to Switzerland. The protective strategies and methods used must also be kept from the prying eyes of adversaries. Our intelligence services are our first line of defence in maintaining Swiss security. Spies from other countries, potential terrorists, nuclear arms dealers and violent extremists should know as little as possible about Swiss intelligence operations.

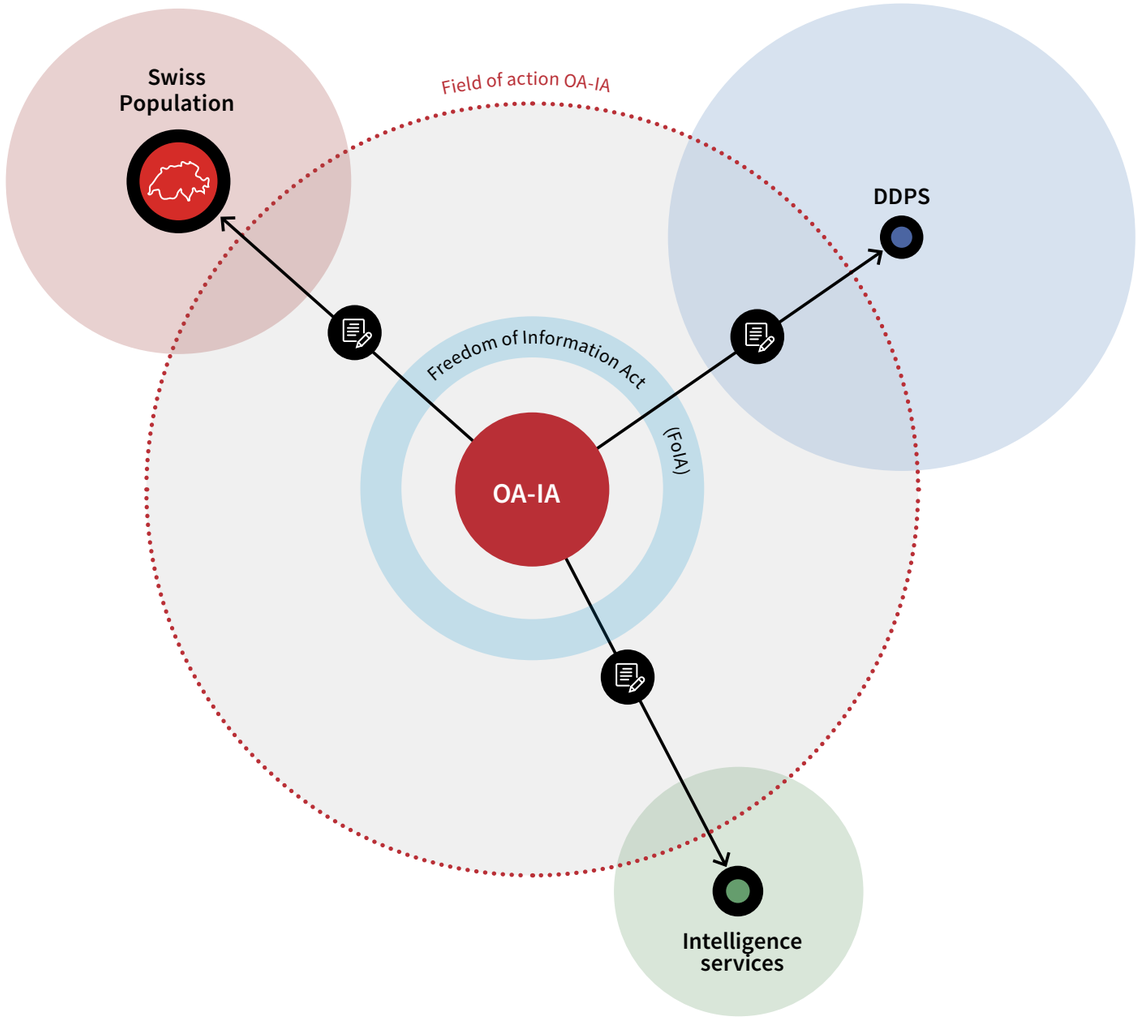
In order to be considered a reliable partner within the international intelligence community and gain access to sensitive and secret information, it is also important that Swiss intelligence activities and strategies remain as far from public scrutiny as possible. If such information were to make front page news, as a result of a secrecy breach, then the intelligence services might find themselves denied access to security-related information exchanged between the various partner intelligence services, thereby exposing Switzerland to subsequent domestic security risks. This is precisely what happened when the Austrian public prosecutor’s office and a police unit under the Ministry of the Interior raided the offices of Austria’s domestic intelligence service, the BVT, and seized numerous data storage media containing classified information. After this incident, the international intelligence community completely lost confidence in the BVT, which has been working to restore its reputation ever since.[5]

Intelligence agencies in general and secret services in particular arouse great mistrust and antagonism among certain segments of the population. This attitude is understandable given the many examples in history of painful and disastrous consequences for ethnic groups, political dissidents or minorities in general. Covert action in the shadows can reinforce existing preconceptions.

The work of an intelligence service consists mainly of gathering and evaluating information. At the same time, stringent legal requirements must remain in place to keep their activities in check. In Switzerland, the work of the FIS was recently tarnished by news reports of obsessive data collection, profiling and wiretapping of Swiss politicians. These reports revived still raw memories of the Secret Files scandal of 1989, when it was discovered that federal authorities and cantonal police

[5] Article published in the NZZ newspaper on 10 April 2019 “Ist Österreichs Geheimdienst noch vertrauenswürdig?” (“Can Austria’s domestic intelligence service still be trusted?”)

Transparent reporting



“The protective strategies and methods used must also be kept from the prying eyes of adversaries.”

“Transparency in reporting makes the field of action of intelligence services clearer and easier to comprehend.”

had been secretly monitoring large swathes of the Swiss population. The FIS is currently working to improve the level of transparency of its work in the eyes of the general public and devotes considerable resources to the handling of requests of access.

The OA-IA is vested with the authority to conduct extensive audits of intelligence activities and Swiss intelligence services are required to be open with the OA-IA. And these agencies have cooperated willingly with the OA-IA in its auditing activities. The extent to which the OA-IA is able to disclose information to the general public is another matter entirely. The general prevailing sentiment within the OA-IA is that the facts surrounding intelligence activities can be explained to a broader public easily and without any lasting detriment to security interests. And it is felt that doing so would encourage greater understanding and ultimately trust in intelligence activities and those working for the Swiss intelligence services.

For example, it is true that the FIS maintains files on political activists in its databases. In most cases, however, these files come from public sources such as press reports and, of course, this information gathering is subject to legal requirements. For example, information on political activities may only be obtained and handled in exceptional cases if there are concrete indications that political rights are being exercised for the purpose of preparing or engaging in terrorist, illegal intelligence or violent extremist activities. During the reporting year, the OA-IA was given access to the FIS file system for the purpose of carrying out random spot checks and assessing how the FIS handled the information gathered about politicians. Its conclusions and recommendations are presented in the present Annual Report.[6]

Auditing and associated reporting activities are not the only means that the OA-IA uses to provide the general public with insight into intelligence activities. The OA-IA is also responsible for handling requests submitted under the Freedom of Information Act (FoIA)[7]. This piece of legislation is intended to enable the general public to gain a clearer understanding of government remits, structures and activities – in this case, those of intelligence services. The OA-IA is aware of this purpose of this legislation and takes this legal mandate seriously. Accordingly, it handled two FoIA requests and describes the experiences in this report.[8]

The OA-IA also helps to maintain transparency by publishing its Annual Report. The OA-IA is legally required to first report to the DDPS before the Annual Report is released to the general public. Although secrecy imperatives mean that specific details must remain undisclosed, we strive to clearly inform the general public of intelligence-gathering activities. First of all, we can explain the reasons why audits were conducted and the methodology used. The clarification of intelligence activities and terminology encourage greater understanding and insight.

The OA-IA is convinced that transparency in reporting makes the field of action of intelligence services clearer and easier to comprehend. This is costly, because the conflicting interests of secrecy and clarity must be carefully weighed up in order to safeguard Switzerland’s security.

Adhering to the requirements set forth in the Freedom of Information Act is a particularly challenging undertaking. In the section that follows, the OA-IA will describe its first experiences with FoIA requests.

[6] Audit report 19-15

[7] CC 152.3
[8] Page 10

“A particular challenge lies in complying with the requirements of the Freedom of Information Act.”

4.2 Freedom of information requests filed in relation to audit reports 18-9 and 18-11

After the press conference on the first annual report, the OA-IA received two freedom of information requests. The Freedom of Information Act (FoIA) is intended to ensure clearer understanding of government remits, structures and activities and open up the filing cabinets and shelves to closer scrutiny. The FoIA request filed by a daily newspaper concerned audit reports 18-9 (Review of the selectors in the system[9]) and 18-11 (Overview of measures to reduce risks in the Military Intelligence Service).

The revised draft of the Intelligence Service Act (IntelSA) initially provided for all FIS activities to be excluded from the scope of application of the FoIA. The Federal Data Protection and Information Commissioner (FDPIC) intervened against this provision in defence of the principle of transparency. In the end, only the most sensitive area of the intelligence service, namely information gathering under Article 67 IntelSA, was excluded from the scope of the FoIA.

Audit report 18-9 deals with the creation, monitoring and adjusting of the selectors used by the EOC to target its information gathering activities. For this reason, the OA-IA denied access to this report citing Article 67 IntelSA. No further action was taken to challenge our decision.

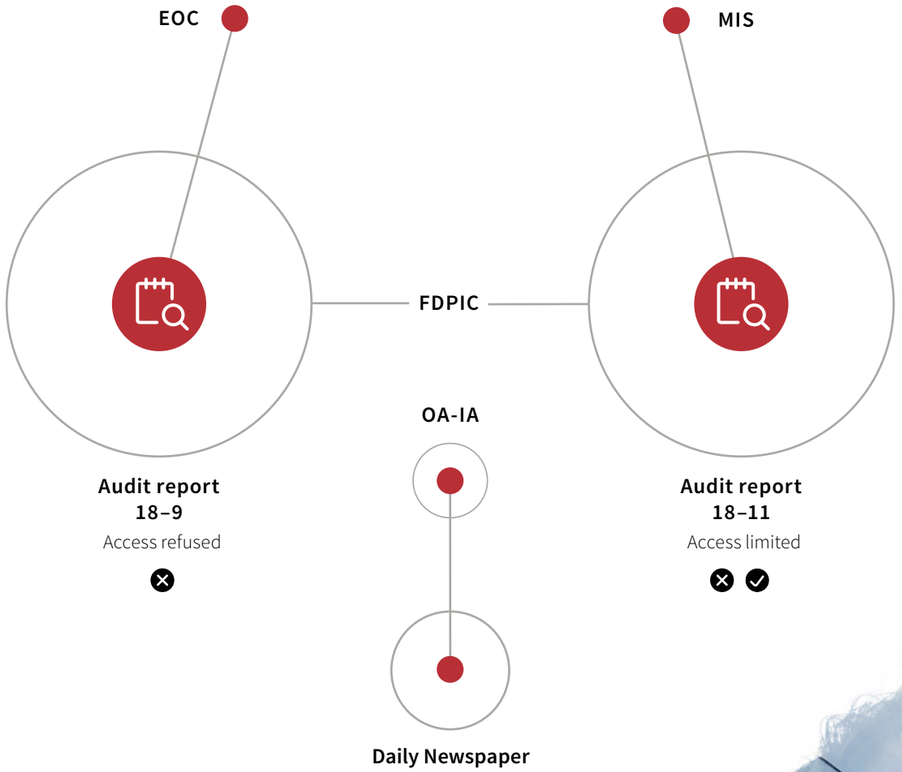
In the case of audit report 18-11, the OA-IA decided differently. Under FoIA provisions, access to government files may be restricted if this puts public security at risk, for example. Information about the structure, activities and strategy of authorities that carry out security-related tasks, in this case the MIS, could be considered as subject to such restricted access. However, the OA-IA did not feel that all of the content of this audit report would put public security at risk if disclosed. We therefore decided to grant access to certain portions of this audit report 18-11 and redacted some of the parts and information contained in it.

Since this report dealt with the MIS as a regulated entity, the OA-IA asked the MIS to take a stance on whether access should be granted. The MIS stated that no part of the report should be disclosed as the report was classified and public disclosure of even redacted portions of the report would compromise the MIS’s ability to carry out its activities. Armed Forces Command supported this position.

At this point, the OA-IA felt the need to legally clarify the various viewpoints and denied access to audit report 18-11 on the basis of the objection raised by MIS. The daily newspaper disagreed with this decision and submitted a request for arbitration to the FDPIC. This is a mediation procedure in which an agreement is sought between the parties, in this case the OA-IA and the MIS, on one side, and the daily newspaper, on the other. During these proceedings, which were presided by the FDPIC, the parties agreed that access could in fact be given to a sizeable portion of the report.

The outcome the arbitration proceedings confirmed the OA-IA’s position of reliably pursuing transparency, understanding and trust wherever possible.

[9] 2018 Annual Report, page 18



5. Oversight activities

5.1 Audit plan

Each year, the OA-IA draws up a risk-based audit plan to structure its tasks. For this purpose, it considers the various audit topics listed in its inventory makes its decisions on the basis of the likelihood of given occurrence and the impact of risks. The audit plan for 2019 included audits in each of the following areas:

- Strategy and planning
- Organisation
- Cooperation
- Information-gathering measures requiring authorisation (IGMRAs)
- Operations
- Resources
- Data processing and storage

The 2019 audit plan was prepared between September and December 2018. During this period, the then head of the DDPS and the supervised authorities were given the opportunity to comment the draft. The final version was then sent to other intelligence oversight bodies for information purposes.

"The counterintelligence unit of the FIS carried out four operations and 170 information-gathering measures requiring authorisation (IGMRAs), making it one of the most active unit within the FIS."

5.2 Audits conducted in 2019

A total of twenty-one audits were planned for 2019. Audits 19-13, 19-15 and 19-16 were further broken down into two or three separate parts, giving rise to a total of seven audit reports. Audit 19-17 "MIS information system landscape" and audit 19-21 "Access to/from third-party information systems (federal level, cantonal level, foreign agencies, law enforcement)" could not be carried out for various reasons and the current prioritisation of tasks. They will be included in future audit plans. 2019 was also the first year in which the OA-IA conducted audits of cantonal bodies. The purpose of these audits was to assess the level of cooperation between FIS and five cantonal intelligence services (CIS).

The OA-IA also carried out internal inquiries, without having to contact the audited bodies. We shall now discuss the various audits conducted in 2019, following the structure of our audit plan.

5.2.1 Strategy and planning

19-1 Counterintelligence strategy

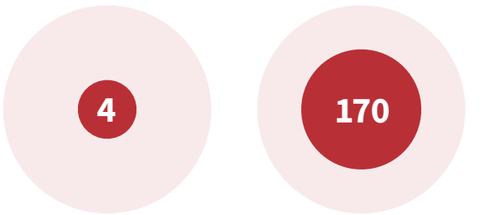
The FIS's Annual Report entitled "Security Switzerland 2019" shows that Switzerland is faced with persistent and increasingly aggressive espionage activities pursued by individual states. In 2019, the counterintelligence unit of the FIS carried out four operations and 170 information-gathering measures requiring authorisation, making it one of the most active unit within the FIS. This was reason enough for the OA-IA to examine the strategic considerations and corresponding measures developed in the area of counterintelligence.

The FIS considers investigating illegal intelligence activities in Switzerland as one of its main tasks. However, the FIS does not have free reign in its counterintelligence activities as it must submit all intended measures through the political system of checks and balances. For this reason, the FIS tends to work more with other authorities on such strategic matters as well as on methodological and organisational aspects. The OA-IA considers current measures to be effective and recommends that other strategic aspects be formulated to a larger extent.

→ Illegal intelligence activities

The term "illegal intelligence activities", also referred to as espionage, is understood to mean all acts aimed at obtaining confidential or secret information for the benefit of a foreign state or a foreign company. In contrast, national "counterintelligence activities" are intended to detect and hinder illegal intelligence activities whenever possible.

Counterintelligence 2019



5.2.2 Organisation

19-2 Management of intelligence data between the defence attaché network and the FIS

In this audit, the OA-IA focused on how information sources abroad are managed and coordinated. The FIS is responsible for gathering intelligence data through the defence attaché network of contacts. Cooperation within the meaning of Article 11 paragraph 2 IntelSA between the Swiss Armed Forces and the FIS is not specified further. The management of defence attachés between the various organisations is documented to some extent. It is essential for the FIS to be able to direct the intelligence missions of defence attachés and this role should therefore be reinforced for greater effectiveness. The added value derived from the intelligence information gathered by defence attachés should also be consolidated further.

5.2.3 Cooperation

Each canton has its own intelligence service (CIS), which exists for the purpose of working with the FIS, in keeping with the provisions of the IntelSA. They may obtain and process information about terrorism, espionage, proliferation, critical infrastructures and violent extremism either at their own initiative or on behalf of the FIS. They are in a way the eyes and the ears of the FIS at cantonal level. These intelligence outposts, which are an integral part of cantonal police forces, are mostly federally funded. Federal subsidies are calculated and paid on the basis of a distribution formula, which is reviewed at three year intervals. In 2018, CIS staff accounted for a total of 124 FTEs.

The OA-IA's oversight remit covers both the activities of the FIS and those of CIS. When planning inspections, it was obvious to the OA-IA that the legality, expediency and effectiveness of cooperation between the FIS and CIS should be examined. At the end of 2018, the OA-IA therefore gave itself the objective of auditing all 26 CIS over the next five years. For this purpose, a standard audit was developed to cover organisational aspects, operations, legality, handling of data, security and use of resources. This also enables comparisons to be made between cantons. In addition to reviewing the relevant documents, audit activities also include an annual survey of FIS employees assigned to work with the audited CIS. OA-IA auditors also visit CIS offices for in-depth discussions that also include representatives of cantonal oversight authorities. Additional meetings are arranged as needed.

→ Defence attachés

Defence attachés form a crisis-resistant, alliance-independent network furthering Swiss security policy interests and the needs of the Swiss Armed Forces. They use and develop this network in a way that ensures that it is an effective and expedient instrument.

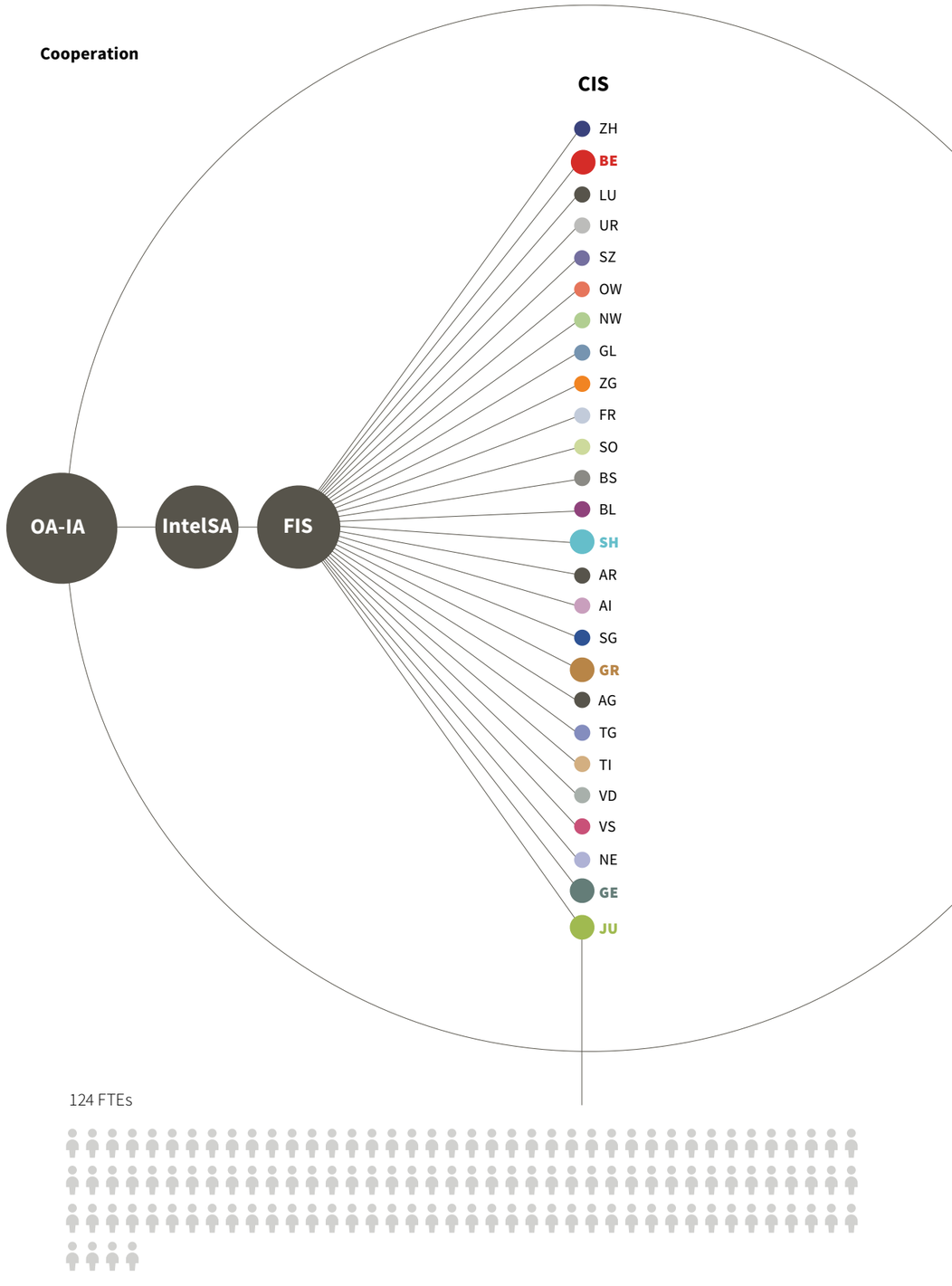
As of 12 August 2019, the defence attaché network was comprised 19 individuals holding primary credentials and 39 individuals holding secondary credentials[10], of which three were inactive due to conflicts (Yemen, Syria and Libya). This network is checked at regular intervals.

The remit of defence attachés is decided by the Federal Council on the basis of the Vienna Convention.

Defence attachés are members of the Swiss Armed Forces. Their orders are formulated by various parties and centrally conveyed by the FIS. Defence attachés are managed by Defence Attaché Operations, which is part of the Armed Forces Staff (ASTAB). The FIS handles intelligence operations.

Defence attachés undergo six months of special training with the Swiss Armed Forces, the FIS and other authorities such as the State Secretariat for Migration (SEM) or the Federal Department of Foreign Affairs (FDFA).

[10] https://www.vtg.admin.ch/de/aktuell/themen/internationale-beziehungen/einsatz.html, last seen on 27 December 2019



19-3 CIS GE

Cooperation between the Canton of Geneva's intelligence service (CIS GE) and the FIS is partially compliant with legislative provisions. However, the Canton of Geneva needs to adjust certain aspects associated with the handling of data to ensure compliance with IntelSA requirements, possibly in cooperation with the FIS. In terms of effectiveness and expediency, the OA-IA found that there was room for improvement in the area of operational cooperation, management of resources and use of technical equipment.

19-4 CIS JU

This audit found that cooperation between the Canton of Jura's intelligence service (CIS JU) and the FIS is fully compliant with legislative provisions.
After the OA-IA noted that CIS JU had rarely gathered information at its own initiative over the past few years, it reminded those responsible of this obligation to do so. On the subject of the expediency and effectiveness of cooperation, the audit revealed that the FIS feedback policy was unsatisfactory. The OA-IA therefore recommended that the cantonal intelligence services should receive feedback on topics such as proactiveness, performance and potential improvements. In order to ensure the protection of CIS JU's own data, the OA-IA calls upon the FIS to provide the cantonal oversight authorities with a detailed explanation of the procedure to be followed when gaining access to intelligence service files within the meaning of Article 11 of the Intelligence Service Ordinance (IntelSO)[11].

19-5 CIS GR

For this audit report, the OA-IA examined cooperation between the Canton of Graubunden's intelligence service (CIS GR) and the FIS. For this purpose, the OA-IA conducted several interviews with FIS employees assigned to work with CIS GR. OA-IA officials also paid a visit to CIS GR offices on 2 July 2019. As of the date of this audit, cooperation between the CIS GR and the FIS is fully compliant with legislative provisions and is both expedient and partly effective. The OA-IA got the impression that the cooperation between the two organizations was established and functioning, apart from the mismatch between the services of the CIS GR and the flatrate compensation paid by the federal government.

The cantons receive a federal subsidy in exchange for the work that they do on behalf of the FIS. The decisive factor is the budget allocation set aside for this purpose in the FIS budget. These federal subsidies to the cantons are based on a distribution formula that takes into account cantonal expenditure. Given the disproportion mentioned earlier, the OA-IA recommended that the FIS and CIS GR reassess together the current situation of mandates and reporting in light of the current federal subsidy. If the cost of CIS GR mandates, reporting and operational services falls below the amount of the federal subsidy, then CIS GR can either provide more operational services to the FIS or the federal subsidy can be reduced. In the same context, the OA-IA also recommended that CIS GR and the FIS explore together the conditions for future and long-term involvement of CIS GR at the World Economic Forum (WEF) Annual Meeting. Foreign delegations taking part in the annual meeting of heads of government and international business leaders in Davos can potentially use this event as an opportunity to engage in espionage.

The FIS makes a considerable effort to encourage cooperation with the CIS, e.g. through the provision of regular training courses, technical equipment and advice. CIS GR benefited from this support and the regular exchange of information. Both sides considered that there was room for improvement in mutual feedback. The OA-IA will therefore monitor further developments in this area.

[11] CC 121.1

19-6 CIS SH

As with the other audits of CIS that the OA-IA conducted in 2019, emphasis was placed on evaluating the level of cooperation between the Canton of Schaffhausen's intelligence service (CIS SH) and the FIS. On 11 April 2019, the OA-IA visited the offices in Schaffhausen and met with the persons involved at cantonal level.

Based on the information gathered, the OA-IA concluded that cooperation between CIS SH and the FIS is fully compliant with legislative provisions and is both expedient and effective. Both sides give importance to the joint accomplishment of intelligence tasks and the positioning of CIS as key partners. CIS SH agreed with the findings in the OA-IA's audit report. CIS SH intends to or has already taken action in response to OA-IA recommendations and advisory notices, e.g. satisfying the IntelSA requirement that records be kept of the deletion of intelligence data from cantonal computer systems after the data have been imported into the FIS computer system.

19-7 CIS BE

The OA-IA visited the offices of the Canton of Bern's intelligence service (CIS BE) on 11 March 2019 for the purpose of conducting its evaluation. OA-IA employees also met with the deputy head of the Canton of Bern's Department of Police and Military Affairs, which is responsible for cantonal oversight. The OA-IA noted a lack of compliance with the IntelSA requirement that records be kept of the deletion of intelligence data from cantonal computer systems after the data have been imported into the FIS computer system. The OA-IA therefore recommended that the head of CIS BE take the necessary action to ensure that intelligence data temporarily kept on cantonal computer systems be deleted within 60 days after the data have been imported into the FIS information system. These clean-ups must be documented.

The OA-IA did not find an irregularities in the cooperation between CIS BE and the FIS. The OA-IA was left with the impression that cooperation between the two organisations is well-established and functional – most likely also due to the geographical proximity.

5.2.4 IGMRAs

→ Information-gathering measures requiring authorisation (IGMRAs)

Information-gathering measures requiring approval encompasses post and telecommunica-tions surveillance, the use of tracking and monitoring equipment in non-public places, hack-ing into computer systems and networks as well as the searching of premises, vehicles or containers. All of these measures enable the FIS to detect threats to Switzerland and its population at an early stage. IGMRAs may therefore only be ordered when there is a spe-cific threat to the domestic or external security of Switzerland relating to terrorism, illegal intelligence service, proliferation of weapons of mass destruction and associated delivery technologies or a planned attack on critical infrastructures. IGMRAs may also be ordered by a decision of the Federal Council if important national interests are at stake. Violent ex-tremism is excluded.

In addition, the use of IGMRAs must be justified by the severity of the threat and satisfy the requirement that other intelligence investigations have thus far failed or would be hopelessly or disproportionately difficult.

IGMRAsmust first be authorised by the Federal Administrative Court (FAC) and then ap-proved by the head of the DDPS, following prior consultation with the head of the FDFA and the head of the Federal Department of Justice and Police (FDJP). The approval bodies must also have access to all information relevant to the case.

For complex cases, several IGMRAs may be needed. For detailed IGMRA statistics, please consult the FIS Annual Report.

19-8 Expediency and effectiveness of IGMRAs

The audit revealed that the FIS used IGMRAs relatively expediently and effectivly. The legal framework for the implementation of IGMRAs is known and the results achieved are in line with expectations. In most cases, the IGMRAs enabled the FIS to confirm or allay suspicions as to whether the individuals targeted constituted a threat or not. However, the human and technical resources required to implement these measures can be optimised further. Instead of a case-by-case solution for language translations, a general practice should be developed.

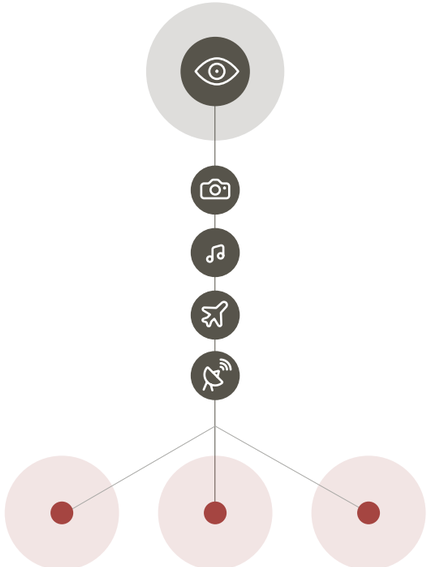
Finally, a legal distinction is drawn between information-gathering measures requiring authorisation and measures that can be implemented without the need for prior approval. The latter are regarded by the legislator as less disruptive, including the observation of people in public and generally accessible spaces. The OA-IA therefore recommends that the FIS becomes better equipped to carry out the necessary observation tasks from the beginning of 2020. In this manner, the order of priority of legally defined information-gathering measures can be maintained. This date corresponds to the planned change in the organisational structure and distribution of observation tasks.

19-9 Implementation of IGMRAs

In audit 19-9, the aim was to determine whether the FIS used IGMRAs appropriately and whether it complied with specified requirements. Around 35 approvals were examined – covering various types of information-gathering activities – to assess whether the IGMRAs in question were implemented in accordance with legislative provisions. The OA-IA also verified whether the conditions imposed at a given time were complied with. During the course of the audit, the OA-IA determined that the FIS approaches implementation of IGMRAs seriously, taking legal conditions and restrictions into account. However, efficient and effective monitoring of the IGMRAs could be further improved to facilitate management and control and more efficient reporting. The OA-IA recommends further development of the skills required to apply, administer and monitor the technical means of implementing IGMRAs.

→ Observation

Observation is an information gathering activity that does not require approval. The FIS uses observation as a means of monitoring events and facilities situated in public and generally accessible locations. Observation may include recording of images and sounds. The use of airplanes and satellites is also expressly authorised. However, protection of personal privacy must be ensured in all cases.



Events and facilities in public and generally accessible places

5.2.5 Operations

19-10 Operations

The FIS considers intelligence operations to be a key element in information gathering. They go beyond day-to-day activities in terms of importance, scope, effort or secrecy. Giving so much importance to intelligence operations as a means of gathering information comes with certain risks:

- Are the available information gathering resources actually being used to address the greatest threats to Switzerland's internal and external security?
- Are legislative provisions being complied with?
- Are the approaches chosen by the FIS in a given operation the most suited means of reaching a given intelligence target?
- How well does the actual outcome of an operation match the desired outcome in terms of scale and quality?

In order to answer these questions, the OA-IA conducts an audit of FIS "Operations" at least once each year.

Based on selected and weighted criteria, the OA-IA established a decision-making matrix and selected eight intelligence operations – four of which already completed – for in-depth analysis and verification. Based on the audit procedures performed, it can be stated that the operations audited are or have been carried out in a lawful, expedient and effective manner. They are clearly defined, limited in time and separately documented.

The introduction of a formal management and control system could help the FIS to improve the overall expediency and effectiveness of operations.

19-11 Human intelligence (HUMINT)

In audit 19-11, OA-IA examined different categories of human sources. The main objective was to determine how the FIS specifically managed human sources. The OA-IA therefore checked the legality, expediency and effectiveness of four selected cases in which the FIS made use of human sources. The protection of sources and persons requires special secrecy in this area; accordingly, HUMINT audits conducted by the OA-IA are classified as SECRET. This audit report will be fully completed in 2020.

→ Operations

In the intelligence field, the term "operation" refers to the gathering of information about related activities in a manner beyond the scope, importance, effort or secrecy associated with normal intelligence gathering activities. An intelligence operation is limited in time. It must also be formally opened and closed.

Intelligence operations may include intelligence gathering activities that do not require approval (e.g. observation in public and generally accessible locations) and IGMRAs (e.g. post and telecommunications surveillance). However, if FIS wishes to carry out IGMRAs this may only take place within the framework of an intelligence operation.

“The OA-IA feels that clearly defined processes and responsibilities would reduce the likelihood of errors and misuse.”

19-12 Protection of sources within the FIS, with emphasis on cover-stories and alias identities

Article 35 of the IntelSA requires the identity of human sources to be protected and kept anonymous. In order to protect life and limb, human sources or persons close to them can receive a coverstory or an alias identity after the conclusion of their cooperation with the FIS. These measures must be approved by the head of the DDPS.

Cover-stories may also be approved by the director of the FIS for personnel working for the FIS or cantonal prosecution authorities. The aim here is to make the employees’ affiliation to their service unrecognisable. These employees can also benefit from alias identities for a limited but renewable period of time if this is necessary to ensure the security of the person concerned or for information gathering purposes.

Cover-stories differ from alias identities in that cover-stories involve the creation or modification of documents (e.g. a diploma) in the name of the person. For false identities, identification documents can be produced or modified – even including fictitious biographical data such as name and date of birth.

It is important to make sure that the FIS also uses these measures lawfully because the production and modification of documents and identification documents is a criminal offence, which will become legally justified by the approval given by the director of the FIS or by the head of the DDPS.

In audit 19-12, the OA-IA sought to determine whether the protection afforded to human sources – particularly the protective means of creating cover-stories and alias identities – was lawful, expedient and effective. The OA-IA noted that the FIS considers the protection of sources to be both an important and serious matter: the FIS protects sources by various means and at different levels. During its audit, the OA-IA found no irregularities in the processes giving rise to the approval of the creation of cover-stories and alias identities. However, all approvals of cover-stories were applied for in advance. This means that they were applied for and approved, but not implemented and used, which in the eyes of the AB-ND was not expedient.

The OA-IA also noted that the processes and responsibilities for requesting, administering, producing, maintaining and winding down cover-stories and alias identities (and the associated cover-story logistics) are not entirely defined and harmonised. The OA-IA feels that clearly defined processes and responsibilities would reduce the likelihood of errors and misuse. At the same time, harmonised processes would enable resources to be used more effectively.

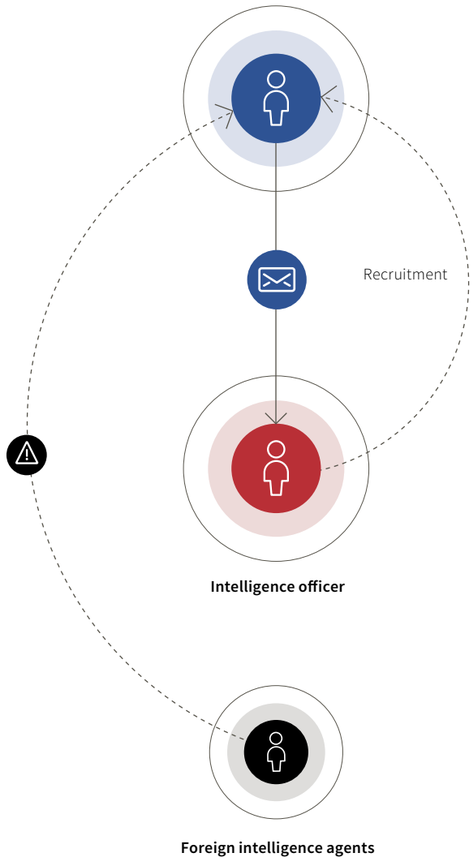
Human intelligence (HUMINT)

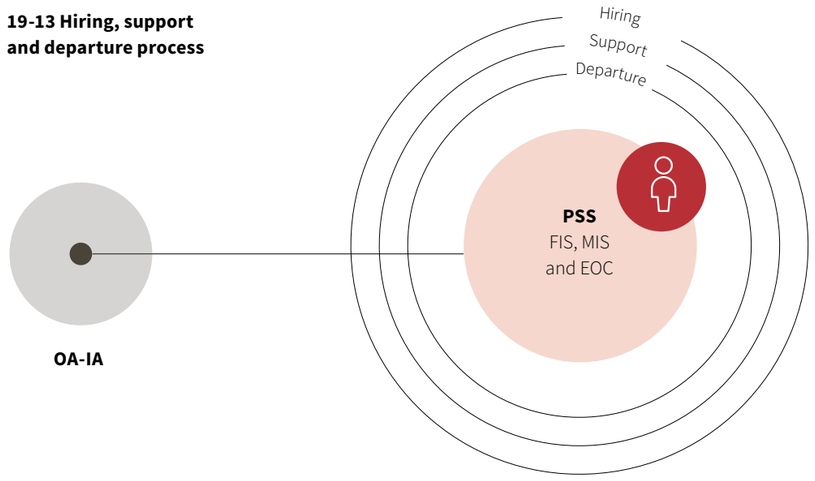
Human intelligence (HUMINT) refers to information gathering by means of interpersonal contact with human sources. Simply put: one person delivers information and another person receives it. The receiving person is an intelligence officer. HUMINT involves taking targeted measures to obtain information in the field either through observation of a person or relying on information provided by a human source.

Human sources are specifically selected and recruited. They must have access to sensitive information and information carriers that are particularly relevant for Switzerland. The protection of sources and persons requires special secrecy. People who work as sources normally provide information to the intelligence services voluntarily, usually knowingly, sometimes free of charge, when it serves their personal or political goals. Target persons for recruitment as a source are especially those who are likely to be able to provide useful information over the long-term. Important criteria are the current access possibilities and professional prospects of a human source. Possible candidates are, for example, employees in the parliamentary sector, representatives of authorities and companies as well as scientists, but also security services personnel. Nevertheless, intelligence officers also use conspiratorial methods to obtain particularly sensitive information.

Foreign intelligence agents also attempt to establish contacts with people who have special knowledge or access to Switzerland. Often foreign intelligence services are established in embassies and consulates of their countries in Switzerland. They themselves - overtly or covertly - pursue information gathering or assist with intelligence operations, which are conducted directly from the headquarters of the services in their home countries. Often they have diplomatic status and benefit from associated diplomatic immunity. If such persons are exposed, they may be deported from Switzerland.

As direct contact, HUMINT remains a fundamental tool for the intelligence services, even if this traditional method has taken a back seat to the use of electronic means. Human sources can also be indispensable in the field ofpolitical espionage, as the main aim here is to obtain information matching the specific requirements of intelligence services.





5.2.6 Resources

19-13 Hiring, support and departure process

A major potential risk associated with intelligence activities are the employees themselves (treason, data theft, espionage etc.). The data theft that occurred within the FIS in 2012 is a specific example. The selection, review, monitoring and support of personnel by HR services and direct superiors are of great importance for risk minimization.

Audit 19-13 was subdivided into two separate sub-audits, the first covering MIS (audit 19-13a) and the second covering the EOC (audit 19-13b), which gave rise to two separate audit reports. The initial intention was to also audit the FIS. However, given the extensive audits already planned for the FIS in 2019, the OA-IA decided to postpone this audit to a later date.

The audit questions related to personnel security screening (PSS) in the three phases of the recruitment cycle: hiring, supporting and departure. The audits, which were based on interviews and analysis of documents as well as on random sampling to check individual process steps, show whether a PSS is carried out for a given process phase and whether this may be considered lawful, expedient and effective.

Well-functioning PSS procedures are in place both at the MIS and the EOC. At the EOC, a large number of positions are subject to the highest level of scrutiny (PSS 12). According to an additional personal interview, PSS procedures are lengthy and time-consuming and must be started at an early stage. In the past, there have been delays in the renewal of expired PSS 12 credentials for long-standing employees. The OA-IA therefore recommended that the renewal process be initiated at an early stage.

The OA-IA compared and analysed the various PSS levels in all three intelligence services (MIS, EOC and FIS). The OA-IA noted that the MIS, EOC and FIS all use of different classification systems to assign PSS levels to employees. This does not make sense from a legal, objective and logical standpoint. These three classification systems need to be reviewed and harmonised in order to improve their effectiveness. This review and harmonisation process should take into account future amendments that may be introduced in the draft revision of the Information Security Act, which was currently being debated in Parliament at the time of the audit.

Results: In the two services audited, sufficient account is taken of the risks in the recruitment process. Usually, the PSS procedure is completed before the person starts his/her first day of work and new employees are then made aware of security aspects and undergo the necessary training.

“In the two services audited, sufficient account is taken of the risks in the recruitment process.”

The risks associated with existing personnel are adequately mitigated and superiors play a key role in identifying changes in an individual’s personal environment. Wherever possible and appropriate, organisational and technical security checks are carried out.

When personnel leave, steps are taken to ensure that entry and access authorisations are disabled or removed. Sufficient attention is paid to the transfer of knowledge and employees leaving the company must sign a confidentiality agreement.

19-14 Secure use of video teleconferencing equipment

Nowadays, video teleconferencing equipment (VTC) is an efficient and widely used means of communication. The FIS operates and uses VTC equipment to provide information to partners.

In most cases, the content of discussions is classified as SECRET. It is therefore essential to prevent data leaks caused by technical flaws in the system or incorrect handling on the part of the user.

To answer the question of whether equipment purchases and use were compliant with legislative provisions, the OA-IA met with FIS employees and selected partners and also analysed existing documentation. Moreover, by observing individual VTC conferences of the FIS, the OA-IA was able to draw conclusions regarding VTC equipment in meeting rooms and how they were used.

The OA-IA audit showed that VTC equipment purchases were compliant with legislative provisions and that VTC equipment was used in an expedient and effective manner, in keeping with intelligence security standards. The OA-IA only found room for improvement in the operation of VTC equipment.

“The OA-IA audit showed that VTC equipment was purchased compliant with legislative provisions and was used in an expedient and effective manner.”

5.2.7 Data processing and archiving

19-15 Operation, content and use of the information systems GEVER FIS, BURAUT data storage and SiLAN data storage (temporary evaluations)

In audit 19-15, the OA-IA examined the operation, content and use of the GEVER FIS[12], BURAUT[13] and SiLAN[14] information systems (temporary evaluations) to determine whether they met legal requirements. Given the extensiveness of the audit and the complexity of GEVER FIS, two audit reports were prepared. Audit report 19-15a is devoted exclusively to GEVER FIS and the two information systems SiLAN and BURAUT were described in audit report 19-15b.

19-15a GEVER FIS

In GEVER FIS, the OA-IA focused on verifying whether the allocation of access rights, collection of data and data retention periods as well as data deletion and archiving satisfied legal requirements. In addition, it checked the effectiveness of installed control systems. To answer the various audit questions, the OA-IA analysed documentation, conducted interviews with employees working at the FIS and the Swiss Federal Archives, and carried out spot checks at the workstations of ten FIS employees.

Information protection and data protection regulations require that FIS employees only access the data they require in order to fulfil their tasks.

[12] System used to manage and control day-to-day tasks
[13] File system used by the Armed Forces Command Support Organisation (AFCSO)
[14] File system used to store data in folders

“The OA-IA found that no files in the GEVER FIS relating to Swiss politicians had been created exclusively on the basis of their political activities.”

The potential consequences of FIS failure to comply with these regulations:

- Threat to Swiss security;
- Lawsuits filed against the FIS;
- Damage to the FIS’s reputation both within the Swiss population and in dealings with partner services.

The OA-IA audit shows that the FIS uses a complex system to allocate access rights in the GEVER FIS system. Various profiles are used to control access. Analysis of the authorisation list and spot checks of ten FIS employees showed that authorisations are adequate and satisfy legal requirements. However, the OA-IA feels that there is still room for improvement in the authorisation management process. Furthermore, the tasks of external agencies providing GEVER FIS maintenance and technical support should also be reviewed.

In GEVER FIS all operationally relevant information must be traceable. This applies in particular to all outgoing intelligence products, and, as with all offices of the Federal Administration, to proof of official activity (answers to letters to citizens, answers to parliamentary initiatives, legislative activities). If operationally relevant information is not saved and processed in a traceable manner in GEVER FIS, then the FIS is unable to justify the information contained in its outgoing intelligence products. In GEVER FIS, no information may be entered or processed on political activities or the exercise of freedom of expression, freedom of assembly and freedom of association.[15] Exceptions: when there are specific indications that the aforementioned rights are being exercised for the purpose of preparing or carrying out activities relating to terrorism, illegal intelligence or violent extremism.

The OA-IA conducted random spot checks to determine the legality of GEVER FIS data entries regarding eleven politicians and verified compliance with the information restrictions laid down in Article 5 paragraph 5 IntelSA. In addition, the OA-IA checked the handling of five requests of access to their personal data filed by private individuals and organisations as well as two politicians who had been the subject of data entries in the GEVER FIS system. The OA-IA audit confirmed that the FIS had responded to the audited information requests properly and completely. The information gathered is essentially compliant with legal requirements. It is also worth mentioning that most of the personal information contained in the GEVER FIS system came directly from press reports. On the basis of audited samples, the OA-IA found that no files in the GEVER FIS relating to Swiss politicians had been created exclusively on the basis of their political activities. For this reason, the OA-IA recommended that the FIS review the legality of the current practice of collecting information from public sources.

So far, there has been no delivery of documents from GEVER FIS to the Swiss Federal Archives (SFA). This is not a problem, however, as the 20-year legal deadline leaves enough time for action to be taken. The OA-IA considers that the FIS practice of delivering files to the SFA on an ongoing basis makes sense, in order not to come under pressure towards the end of the legal retention periods.

The audit report will not be completed and sent to the head DDPS until the first quarter of 2020.

19-15b SiLAN / BURAUT

SiLAN is a protected internal IT platform used by the FIS to process data at all classification levels up to SECRET. Among other things, a data storage system is operated in this network, enabling temporary evaluations to be processed. The OA-IA audit was intended to determine whether this data storage system was being used in accordance with legislative requirements.

During an on-site visit, the OA-IA examined the rights granted to ten FIS employees to gain access to the temporary file storage system. The audit showed no unnecessary and unjustified access authorisations. Analysis of the contents in the temporary data storage system revealed no conspicuous features or violations of applicable regulations. The processed data were not older than the five-year maximum data retention period. In the OA-IA’s view, yearly evaluation by the FIS quality assurance unit combined with the necessary approval by the data owner ensure adequate control of compliance with legal requirements. Since the audits 18-1 and 18-2, the FIS had continuously continued and improved the measures taken in this respect.

FIS employees also have a BURAUT workstation in addition to the SiLAN environment. BURAUT is a standard platform used by the Federal Administration and is run on an AFCSO server[16] . In exceptional cases, and subject to approval by the Head of Information Management, it serves as a storage system for data exchanged between federal offices and departments involved in inter-agency cooperation projects. Since these data are handled outside the protected FIS network, they are less well protected against unauthorised access. Therefore, no unencrypted, CONFIDENTIAL or SECRET information may be processed in the BURAUT environment.

The OA-IA feels that the clean-up operation carried out by the QS FIS was successful and has led to greater awareness and a significant reduction in data storage.

19-16 Classification of information

Audit 19-16 was conducted for all three intelligence agencies, namely FIS, MIS and EOC. The main purpose was to verify whether physical and electronic data was handled in accordance with legislative provisions.

The issue of classification of information broaches other topics and therefore cannot be considered in isolation. For example, the handling of classified information touches upon aspects of information security and physical safety.

[15] Article 5 paragraph 5 IntelSA

[16] Armed Forces Command Support Organisation (AFCSO)

→ GEVER

In Switzerland, GEVER (GEschäftsVERwaltung) is the name given to the electronic records and process management system used by the Federal Administration. GEVER serves as the foundation for e-Government.

Since GEVER was introduced within the Federal Administration, all information relating to day-to-day tasks is exchanged and stored electronically. This includes files that government agencies handle as part of their legal mandate.

GEVER is guided by operating procedures. At the same time, it enables transparent, traceable, legally compliant and efficient file management. The lifecycle of managed documents from their creation to their use, storage, segregation, archiving or destruction are all shown in GEVER.

“The issue of classification of information broaches other topics and therefore cannot be considered in isolation.”

Information security

Social, economic, political and governmental spheres are increasingly influenced by the availability of networked data. It is therefore essential that this information be sufficiently protected in an economically viable manner. This applies not only to the data itself, but also to the information and communication systems that capture, process, transmit or store the data. In this context, we refer to information security, which combines the notions of information protection, IT security and data protection.

Information protection

This term refers to the protection of information used by the Federal Administration and the Swiss Armed Forces, in particular the classification and processing of this information. By classification, we mean that information is assigned a category that indicates the level of protection required (SECRET, CONFIDENTIAL or INTERNAL). Protecting information means ensuring that it remains undisclosed, unaltered, accessible and traceable.

The OA-IA noted a certain a lack of terminological and conceptual clarity in the use of terms. This can lead to confusion: on the one hand we have an “Information Protection Ordinance” and at the same time “information security management systems” (ISMS). Parliament is currently working on a new “Information Security Act”. The latter is currently undergoing legislative review and is expected to remove uncertainties.

Audit 19-16 (Classification of information) was carried out for the FIS, MIS and EOC to ensure that physical and electronic information is handled lawfully and in accordance with the relevant information protection requirements. The OA-IA noted that federal information protection aspects for each service are clearly dictated by the DDPS.

With a comprehensive, well-documented and active ISMS, the FIS ensures that information is handled lawfully, on the one hand, and that all information security requirements are met, on the other. At the MIS and EOC, information security processes are outlined to a certain degree in individual concepts, handbooks and presentations. The OA-IA expects that this situation will improve once the EOC’s own ISMS has been rolled out at Commando Operations (Cdo Op) in mid-2020.

Within the secure environment of internal information systems, the distinction drawn between whether the disclosure of information to unauthorised persons is detrimental (INTERNAL), damaging (CONFIDENTIAL) or very damaging (SECRET) to national interests is less important. However, outside the secure ISMS environment, classification as CONFIDENTIAL or even SECRET entails corresponding additional administrative effort. Authors of classified information must be aware of this fact and make measured use of classification categories. If the balancing act between the need to protect information and unnecessary additional workload is not achieved, there is a risk that chronic over-classification of documents will ultimately lead to classification no longer being taken seriously. The original intention of classifying information that is actually worth protecting can thus be lost or at least diluted. In order to ensure a certain standard and thus comparability within the organisation with regard to classification, random checks could be carried out regularly, for example. These random checks should be carried out by a body not involved in the core activities of the unit in question.

“EOC information systems must be continuously updated.”

19-18 EOC information system landscape

The EOC is part of the Swiss Armed Forces and performs a range of technical tasks on behalf of the Swiss Armed Forces as well as on behalf of the military and civilian intelligence services. One area of activity is communications intelligence (COMINT), which includes the interception of voice communication via satellite phones or the interception of data communications via terrestrial cables. Another area of activity is cyberspace, which includes both defensive and offensive cyber capabilities and cyber intelligence operations.

The OA-IA therefore wanted to know which information systems were being used at the EOC for its intelligence activities. The OA-IA felt that this topic was important since only a clear identification of these information systems would enable reliable conclusions to be drawn regarding other areas of interest such as the question of data management.

The OA-IA audit showed that the information systems are well-documented. Operation is based on a solid legal framework and the EOC goes to great lengths to protect the systems against unauthorised external access.

New, constantly changing communication technologies, the diversity of communication channels and the huge volumes of data generated pose major challenges for the EOC. The information systems and legal bases must therefore be continuously updated in order to meet the needs of service recipients such as the FIS or the MIS.

19-19 Data analysis tools in the EOC

This audit was not started until the end of December 2019, and therefore this report does not provide any information on this.

19-20 Disclosure of personal data to foreign authorities (Article 61 IntelSA)

The FIS exchanges information with foreign partners on a daily basis, which is why the OA-IA decided to audit this aspect. The transfer of personal data to foreign authorities is expressly regulated in Article 61 IntelSA.

The audit showed that the circle of persons involved in the exchange of information is clearly defined, that processes are in place for the various communication channels with foreign partners and that the exchanged messages are recorded and easily accessible. The interviews conducted and random sampling of some thirty reports sent to foreign partners showed that the practice followed by the FIS generally enables compliance with legal requirements. However, compliance with these requirements seems to be the result of routine rather than an active awareness of the applicable legal requirements. The OA-IA therefore recommends that the FIS take various measures to make employees more aware of legal requirements, such as the adaptation of internal guidelines and/or regular training of the employees concerned. These measures should enable the FIS to ensure that the lawful disclosure of personal data abroad is also guaranteed in the future.

The OA-IA also noted that data transferred to third parties must come from the IASA FIS information system. FIS employees are aware of this requirement and comply with it. In the case of disclosure of information relating to operations, it can sometimes take a few days before messages are entered into the relevant information system. The FIS is aware of this issue and has already begun allocating additional resources for the coming years to enable messages to be sorted, thereby mitigating this problem. In the meantime, it is the responsibility of the FIS to do everything possible to ensure compliance with legislative provisions.

5.3 Acceptance

According to Article 78 paragraph 6 IntelSA, the OA-IA shares audit results with the DDPS and can make corresponding recommendations. In addition to these recommendations, the OA-IA may also issue advisory notices to audited parties.

According to OA-IA practice, there are two cases where advisory notices are given:

1) Findings where optimisation does not have to be implemented by the head of the DDPS as the appropriate level but rather at a lower operational level (e.g. bringing cell phones at meetings where confidential information will be discussed).
2) Findings where the audit reveals unexpected circumstances that were not directly covered by the audit mandate but are nevertheless of a certain relevance.

OA-IA advisory notices are not legally binding and the OA-IA does not take any steps to verify implementation. Advisory notices are an important methodological tool used to identify future audits. Since the decisions, specifications or work of external bodies have an impact on intelligence activities, advisory notices (and recommendations) may also concern bodies that are not subject to OA-IA oversight.

Under Article 78 paragraph 7 IntelSA, the DDPS is responsible for ensuring that OA-IA recommendations are implemented. It therefore orders the supervised bodies to implement OA-IA recommendations. Although OA-IA advisory notices are not binding, the DDPS usually requires the audited bodies to also take OA-IA advisory noticess into account. In 2019, the OA-IA formulated 63 recommendations and issued 40 advisory noticess. All of its recommendations were adopted.

During their work, the auditors were received constructively and professionally by all audited bodies. They were given access to all documents and information systems needed to carry out the audit tasks. Staff also remained at the disposal of the auditors. The interviews were scheduled and conducted in a timely manner and answers to additional questions were provided promptly.

5.4 Controlling of recommendations and advisory notices

Legislation on intelligence activities does not expressly cover verification of implementation of recommendations. In consultation with the DDPS and the audited authorities, it was agreed that the DDPS would include the OA-IA in the distribution list of internal memos on implementation of OA-IA recommendations and consideration given to OA-IA advisory notices. In 2019 the first deadlines for implementation of OA-IA recommendations expired. The OA-IA's internal notification and review process can be optimised further. At present, no reliable statements can yet be made on the number and, above all, the qualitative aspects of implemented recommendations. In 2019, 40 of these recommendations are slated for formal implementation and 26 recommendations have already been implemented. In the event that the OA-IA is not entirely satisfied with action taken to implement its recommendations, it may check them in subsequent audits.

6. Insights from inside

6.1 Revision of IntelSA

In the reporting year, the DDPS was asked to begin work on revising IntelSA. On 27 August 2019, the FIS invited representatives of the federal and cantonal bodies concerned to a first meeting, where various working groups were set up. Three OA-IA employees took part in the "Surveillance" working group, otherwise, one representative of the Independent Control Authority for Radio and Cable Communications Intelligence (ICA) and one representative of the GS-DDPS are also members of this working group.

The FIS was asked to consider proposed amendments to Article 142 paragraph 2 and paragraph 3 of the Parliament Act (ParlA)[17] in connection with 77-79b IntelSA. On 3 December 2019, the OA-IA attended the final meeting of this phase of the legislative project. In addition to formal changes to the budgeting process, key aspects were the merging of ICA and OA-IA and the creation of a legal basis for the OA-IA to engage in international activities.

[17] CC 171.10

6.2 Continuing training of OA-IA employees

In 2019, OA-IA employees attended symposiums on the topic of information security and data protection as well as individual training courses, particularly in the area of risk management.

In addition, the OA-IA held internal training courses for its team in the following areas:

- Counterintelligence
- IGMRAs
- Interviewing techniques and tactics
- Presentation of FIS GEVER information system
- Refresher course on emergency aid
- Data protection
- Presentation of IASA information system

The various events were organised by FIS in-house experts as well as external partners such as the Personnel Security Screening unit of the DDPS or the FDPIC. The OA-IA would like to take this opportunity to thank the various parties involved for their support.

"Transparency is a basic attitude and not a project."

7. Coordination

7.1 National contacts

A key part of OA-IA's remit is the coordination of oversight activities. It therefore also exchanged views with national authorities and other oversight authorities in 2019.

Control Delegation (CDel)

The CDel invited the OA-IA to hearings on 23 January 2019, on 12 April 2019 and on 23 October 2019. At these hearings, the OA-IA reported to the CDel regarding the audit reports conducted in 2018 and 2019 (18-5 Operations management – Management cycle, 19-12 Protection of sources within the FIS, with emphasis on cover-stories and false identities) and its first Annual Report.

The CDel invited OA-IA representatives to attend a conference in Bern on 26 February 2019, which included representatives of parliamentary oversight bodies from 21 cantons. The OA-IA was given the opportunity to present its audit activities of cantonal intelligence services.

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

On 4 January 2019, a meeting was held between the head of the OA-IA and the head of the ICA. Among other things, they discussed future challenges associated with oversight activities relating to cable communications intelligence. The coordination of oversight and auditing activities will take place at bilateral level whenever necessary.

Federal Administrative Court (FAC)

The Division 1 of the Federal Administrative Court (FAC) decides on IGMRA and cable communications intelligence requests submitted by FIS. The exchange of experiences with this institution is important to OA-IA, even if the court is not subject to its oversight. The OA-IA and the FAC therefore held a bilateral meeting to exchange experiences on 30 January 2019 and on 2 October 2019.

Enquiries from the public

In 2019, the OA-IA received eight enquiries from citizens, including from students wishing to know more about oversight activities and from individuals who felt upset or threatened by alleged intelligence activities. The OA-IA can use the information that it receives in its audit activities. It may, for example, check whether a described action can be attributed to a service and, if so, whether this action was lawful. For example, the information obtained by the association "grundrechte.ch" was considered and integrated in audit 19-15 a (GEVER NDB). However, the OA-IA is not a complaints body and accordingly has no authority to inform an individual of any findings that may affect him or her. The FDPIC may be contacted to find out whether any data concerning individuals are processed lawfully and whether the delay of access is justified.

The head of the OA-IA met with the following individuals in 2019:

- Head of DDPS Viola Amherd (19 March, 29. August)
- Secretary General DDPS (6 May)
- Director of FIS (12 March 11 June, 4. October and 29 November
- Head of MIS (12 February, 28 June and 1 October)
- Head of EOC (9 January)
- FDPIC (16 January)

7.2 International contacts

Intelligence services routinely share information and data across national borders and do so in a particularly intensive manner with partner services. In contrast, the bodies responsible for overseeing intelligence services generally find their authority limited to national borders. National oversight bodies also feel that international cooperation with their counterparts in other countries is important. By exchanging experiences and auditing methods and comparing the results obtained and conclusions drawn, oversight bodies become more familiar with one another and gain a clearer understanding of their day-to-day activities.

“Being transparent does not mean sharing every detail.”

Oversight Network Meetings in The Hague, Brussels and Copenhagen

The Hague, 24 January 2019

Representatives of intelligence service oversight bodies from Belgium, Demark, the Netherlands, Norway and Switzerland met in The Hague to explore the possibility of joint oversight projects – including the use of PNR data[18] by intelligence services. The OA-IA did not actively participate in the project but could benefit from the exchange. The oversight bodies also discussed innovations in technical and electronic oversight. Specifically, the focus was on how, for example, information systems from intelligence services can be efficiently supervised.

Brussels, 7 March 2019

In addition to the representatives who attended the meeting in The Hague, two representatives from the British oversight body were also present. All of the delegations agreed that future cooperation requires a well-balanced and reasonable growth in network membership and in the frequency of international meetings. In addition to discussing the composition of the network, participants examined an oversight method referred to as “system-based oversight”. While not intended to replace other more classical forms of oversight such as in-depth investigation, system-based oversight would offer the advantage of being based on a yet to be developed international auditing standard, which would facilitate cooperation between oversight bodies. Without such a standard, system-based oversight could not be adapted to national contexts. In some of its own audits, the OA-IA already uses system-based oversight; e.g. audit 18-10 “Overview of FIS measures to reduce risks, incl. the work done by the Federal Intelligence Service (FIS) with cantonal intelligence services (CIS)”. The network will continue discussions of this topic in the future.

Copenhagen (27 June 2019)

The network continued its efforts towards system-based oversight and discussed possible common standards for this type of oversight. Using specific examples, the participants exchanged experiences and best practices, especially in the areas of risk assessment, mapping of IT and data infrastructure or technical solutions for oversight. The representatives of participating oversight bodies held four workshops to discuss possible common standards in these areas. For the first time, oversight bodies from Germany and Sweden were represented in the network with observer status.

European Intelligence Oversight Conference 2019 (The Hague, 12 December 2019)

The European Intelligence Oversight Conference was devoted to the objective of “improving oversight of international cooperation between intelligence agencies”. The participants discussed topics such as future challenges for international oversight of intelligence services or multilateral oversight standards.

Additional contacts

OA-IA employees also took part in the 3rd symposium on the networking of intelligence services and corresponding legislation, which was held in Berlin on 7/8 November 2019.

[18] PNR refers to personal data collected and stored by airlines. Such data includes, for example, the name of the passenger, email address, date of birth, passport information, travel dates or itineraries.

8. A view from outside (carte blanche)

The Annual Report should also include an outsider’s perspective on the subject of transparency, which on this occasion is given by Martin Stoll.

Parked in the shadows

Often my informants went to great lengths to protect secrecy. Our clandestine meetings took place according to a meticulously planned script. While walking to the agreed meeting point, I was observed (to make sure that nobody was following me). Sometimes there were documents placed in an anonymous dropbox. Other times it was a long walk through a forest or an hour-long drive. Cover names were agreed upon and communication channels established. It was a bit like in the movies.

My informants had every reason to be cautious. The employees of Swiss intelligence and secret services would have lost their jobs or pensions if their contacts with me had become known.

This is how the South Africa affair of the then Foreign Intelligence Service came to light. Behind the back of Swiss diplomatic efforts to end the apartheid regime, the Swiss military maintained questionable relations with intelligence services in the Cape, and it became known that a pilot with the International Committee of the Red Cross (ICRC) had been hired as a spy by the Swiss intelligence service in Angola. It could also be confirmed that the intelligence service had stolen espionage files in 1982 while occupying the Polish embassy in Bern in an operation that was illegal under international law.

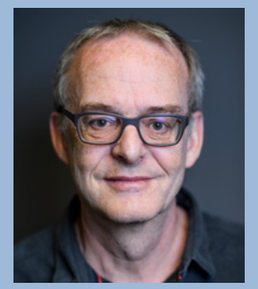
These were highly controversial political events, which show that the intelligence service, which at that time was part of the military establishment, knew virtually no taboos.

In recent years, I was told how an IT specialist from the Federal Intelligence Service (FIS) had copied huge amounts of confidential and secret information. Only at the last minute was the man, who had felt bullied and wanted to sell the data, stopped after a tipoff from a major bank. I was told that the FIS had temporarily suspended the long-time employee. It was the prelude to the affair surrounding the Zurich private investigator Daniel M., who was commissioned by the FIS to spy on financial authorities in Germany.

For members of the press, secret service leaks are a stroke of luck.

In the vast majority of cases, the informants had honourable motives. They were people who were concerned about “the service”. In the eyes of the informants, something was getting out of hand - and no one was there to correct it.

The headlines were followed by parliamentary investigations and oversight reports. These reports brought the processes that had got out of hand back to Helvetian normality. This is a necessary and important process for intelligence services, which (rightly so) sometimes operate on the edge of legality.



Martin Stoll (*1962) has worked as an investigative journalist for the past 35 years. Back in the 1990s, while working as a correspondent for the Tages-Anzeiger, he investigated the red light scene in Zurich and uncovered a clandestine connection between the Swiss intelligence service and the Apartheid regime in South Africa. While working for the “Sonntagszeitung”, he launched the research desk. He is the founder and CEO of a foundation called Öffentlichkeitsgesetz.ch, which advocates transparency in government. He has also worked as a news correspondent specialised in the Federal Administration for the Sonntagszeitung and as a research trainer. Finally, he is vice president of the journalists’ association investigativ.ch.

From a media representative's perspective, the inside information I received was a stroke of luck. In Switzerland, public outrage is easy to control when it comes to secret service material. Even the most harmless spy stories have readers hooked. And they are very likely to shake their heads and say, "Look what the intelligence service has done once again."

One could scold the media claiming unjust motives: self-interest, maximising sales, unnecessary muckraking. Of course, we want to be successful - also with our readers. However, it is also our task and passion to investigate, pierce the veil of secrecy and denounce abuses.

However, the strategy that the Federal Intelligence Service has adopted in dealing with this critical public is wrong. Today the FIS does everything it can to avoid attracting attention. It pulls away, observes - and acts helplessly when it is in the spotlight. The intelligence service should urgently ask itself: Why do we have our backs against the wall so quickly when an incident occurs? Why it is that even with reasonable explanations, the troubled waters cannot be calmed?

Affairs and scandals make it clear that even thirty years after the Secret Files affair, the Federal Intelligence Service still has not managed to foster acceptance and appreciation from its client - the public - for the work that it does. The public does not know what intelligence services are good for, what their task is, what their benefits and freedom of action are.

This is also due to the short-sighted transparency policy of the FIS in recent years. The promise made by Federal Councillor Adolf Ogi - when he announced "Glasnost in the Pentagon" after the bizarre affair involving the intelligence service accountant Dino Bellasi in 2001 - remains a political joke to this day.

Excessive reluctance on the part of the FIS to engage with the public damages its reputation

The fact that the Federal Intelligence Service scoffs at the notion of openness is made clear by statistics on implementation of the Freedom of Information Act (FoIA). This legislation gives citizens and thus also members of the press the opportunity to inspect the files of the Federal Administration. The aim of the FoIA is to improve the public's understanding of the work of the Federal Administration. And the FIS is also subject to this legislation. However, from 2012 to 2018, of the total of 62 media professionals, non-governmental organisations and citizens that submitted freedom of information requests to the FIS, only 8 were granted access to an unredacted document and 33 requests were completely dismissed by the FIS's legal service. This is an extremely meagre track record from the citizens' and media perspective.

In order to understand the FIS's transparency policy, I submitted a FoIA request back in 2014 to gain access to the FIS's records of incoming FoIA requests from the previous three years. I was pleased to receive the anonymised documents. However, most of the sixteen FoIA requests had been denied with the blanket statement that domestic or foreign security would be jeopardised by publication.

When the intelligence service so consistently places itself in the shadows and does not allow any scrutiny, it damages its own reputation. This is illustrated by an example from the series of proposals that I was able to see and which concerned a subject that I was very familiar with. 23 years after the fall of the Berlin Wall, an applicant requested access to the "Walter B. file". B. alias "Max" was one of the most important spies working for Switzerland during the Cold War. The then driver at the GDR Embassy was recruited by Swiss counterintelligence officers after he was caught shoplifting at a department store in Bern. Subsequently, B. gave Switzerland deep insight into the operations of Eastern intelligence services for many years. Although "Max" had told me his story in long conversations, and although the files and video records of the GDR State Security Service (Stasi) are publicly accessible in Berlin ("Max" was later arrested and convicted in East Berlin), the FIS denied the FoIA request. Thus, it missed a golden opportunity to contribute to analysis of this exciting piece of contemporary history and thus to legitimise risky intelligence work.

The fundamentally publicity-adverse attitude was also evident when the FIS, with the new Intelligence Service Act, sought to exempt itself from the principle of transparency in the operative arena. A completely unnecessary action (secrets can also be effectively protected with FoIA) and this was yet another missed opportunity: the FIS would not have to be secret in principle, but rather as transparent as possible so that it would be able to explain its work plausibly.

As a result, the intelligence service will continue to be judged solely on the basis of its mishaps and failures. Sooner or later, the over-classification mindset cultivated today will fly back into their faces like a boomerang. Because one thing is certain: it is only a matter of time before the next intelligence scandal emerges.

9. Key figures as of 31.12.2019

Staff

1.1.2019	**9**
31.12.2019	**10**
Departures	**0**

Audits

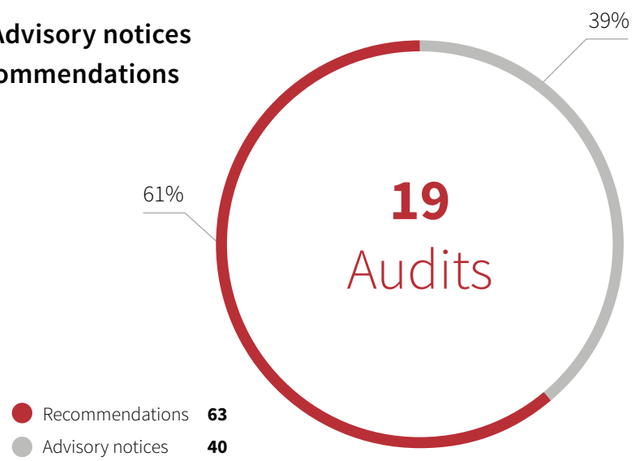
Planned audits	**21**
Unannounced audits	**0**
Completed Audits	**19**

Number of interviews conducted in 2019 **119**

Budgeted workforce

10 full-time positions

Audits, Advisory notices and Recommendations



10. Annex

10.1 2019 Audit Plan

No	Name of audit	Agency audited
19–1	Counterintelligence strategy	FIS
19–2	Management of intelligence data between the defence attaché and the FIS	FIS
19–3	CIS GE	CIS GE
19–4	CIS JU	CIS JU
19–5	CIS GR	CIS GR
19–6	CIS SH	CIS SH
19–7	CIS BE	CIS BE
19–8	Expediency and effectiveness of IGMRAs	FIS
19–9	Implementation of IGMRAs	FIS
19–10	Operations	FIS
19–11	Human Intelligence (HUMINT)	FIS
19–12	Protection of sources within the FIS, with emphasis on cover-stories and alias identities	FIS
19–13	Hiring, support and departure process	MIS, EOC
19–14	Secure use of video teleconferencing equipment	FIS
19–15	Operation, content and use of the information systems GEVER FIS, BURAUT data storage and SiLAN data storage (temporary evaluations)	FIS
19–16	Classification of information	FIS, MIS, EOC
19–17	MIS information system landscape	MIS
19–18	EOC information system landscape	EOC
19–19	Data analysis tools in the EOC	EOC
19–20	Disclosure of personal data to foreign authorities (Article 61 IntelSA)	FIS
19–21	Access to/from third-party information systems (federal level, cantonal level, for-eign agencies, law enforcement)	FIS
19–22	Controlling of recommendations	FIS, NDA, EOC

10.2 List of abbreviations

AFCSO	Armed Forces Command Support Organisation
BE	Canton of Bern
BURAUT	Data storage system
BVT	Domestic intelligence service of Austria
CC	Classified Compilation
CDel	Control Delegation
CIS	Cantonal intelligence service
COMINT	Communications intelligence
DDPS	Federal Department of Defence, Civil Protection and Sport
EOC	Electronic Operations Center
FAC	Federal Administrative Court
FDFA	Federal Department of Foreign Affairs
FDJP	Federal Department of Justice and Police
FDPIC	Federal Data Protection and Information Commissioner
FIS	Federal Intelligence Service
FoIA	Federal Act on Freedom of Information (Freedom of Information Act, CC 152.3, FoIA)
FTEs	Full –time equivalents
GE	Canton of Geneva
GEVER	Electronic records and process management system used by the Federal Administration
GR	Canton of Graubünden
GS	General Secretariat
HUMINT	Human intelligence, Obtaining information from human sources
IASA	Integrated analysis system of the FIS
ICA	Independent Control Authority for Radio and Cable Communication
ICRC	International Committee of the Red Cross
IGMRA	Information gathering measures requiring authorisation
IntelSA	Federal Act on the Intelligence Service (Intelligence Service Act, CC 121, IntelSA)
IntelSO	Ordinance on the Intelligence Service (Intelligence Service Ordinance, CC 121.1, IntelSO)
ISMS	Information Security Management System
JU	Canton of Jura
MIS	Military Intelligence Service
NZZ	Neue Zürcher Zeitung
ParlA	Federal Act on the Federal Assembly (Parliament Act, CC 171.10, ParlA)
PNR	Passenger Name Record
PSS	Personnel security screening
OA-IA	Independent Oversight Authority for Intelligence Activities
QS FIS	Quality assurance body of the FIS
SEM	State Secretariat for Migration
SFA	Swiss Federal Archives
SH	Canton of Schaffhausen
SiLAN	Data Storage System
VTC	Video teleconferencing equipment
WEF	World Economic Forum

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