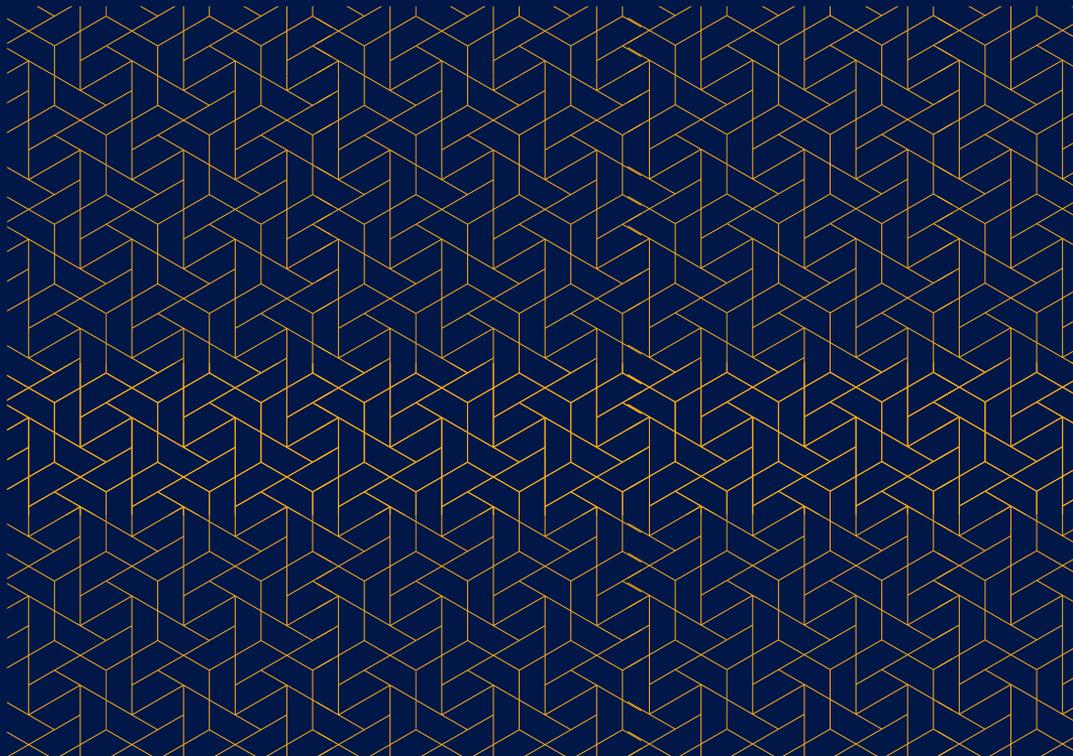


THEMATIC BRIEF

**INTELLIGENCE
PROCUREMENT**



About this Thematic Brief

This Thematic Brief was prepared by DCAF's Europe and Central Asia Division. DCAF would like to thank the Federal Department of Defence, Civil Protection and Sport (DDPS) of the Swiss Confederation and the Norwegian Ministry of Foreign Affairs for its generous support in making this publication possible.

About DCAF

DCAF - Geneva Centre for Security Sector Governance is dedicated to improving the security of states and their people within a framework of democratic governance, the rule of law, respect for human rights, and gender equality. Since its founding in 2000, DCAF has contributed to making peace and development more sustainable by assisting partner states, and international actors supporting these states, to improve the governance of their security sector through inclusive and participatory reforms. It creates innovative knowledge products, promotes norms and good practices, provides legal and policy advice and supports capacity-building of both state and non-state security sector stakeholders.

Copyright

Published in Switzerland in 2021 by DCAF - Geneva Centre for Security Sector Governance

DCAF - Geneva Centre for Security Sector Governance

Maison de la Paix

Chemin Eugène-Rigot 2E

CH-1202 Geneva, Switzerland

Tel: +41 22 730 94 00

info@dcaf.ch

www.dcaf.ch

Twitter @DCAF_Geneva

Cite as: DCAF - Geneva Centre for Security Sector Governance, 2021. Intelligence Procurement. Thematic Brief (Geneva: DCAF).

Note

The opinions expressed in this publication are those of the authors and do not reflect the opinions or views of the Federal Department of Defence, Civil Protection and Sport of the Swiss Confederation and the Norwegian Ministry of Foreign Affairs.

DCAF encourages the use, translation, and dissemination of this publication. We do, however ask that you acknowledge and cite materials and do not alter the content.

Copy-editor: Alessandra Allen

Design & layout: DTP Studio

ISBN: 978-92-9222-619-0

Table of Contents

List of Abbreviations and Acronyms	4
Introduction.....	5
Key Concepts and Definitions	6
Regulatory Frameworks for Intelligence Procurement.....	7
1. Intelligence Procurement versus Public Procurement: At What Point Do Special Procedures Apply and Public Procurement Laws Do Not?	9
2. Intelligence Procurement: Features, Exemptions, and Special Procedures	11
2.1 Selection of specific providers and foreign contractors	12
Security clearance	12
Foreign contractors	14
2.2 Limiting competition and transparency	14
2.3 Decentralized management.....	15
2.4 Inter-agency cooperation	16
3. Oversight of Intelligence Procurement	17
3.1 Internal oversight.....	17
3.2 External oversight.....	17
Audit office.....	18
Parliamentary oversight	19
Public oversight.....	21
Recommendations	22

List of Abbreviations and Acronyms

ABW	Internal Security Agency - Agencja Bezpieczeństwa Wewnętrznego (Poland)
AW	Foreign Intelligence Agency - Agencja Wywiadu (Poland)
BND	Federal Intelligence Service - Bundesnachrichtendienst (Germany)
CVFS	Special Funds Verification Committee - Commission de Vérification des Fonds Spéciaux (France)
DGSE	General Directorate for External Security - Direction générale de la sécurité extérieure (France)
DGSI	General Directorate for Internal Security - Direction générale de la sécurité intérieure (France)
DRM	Directorate of Military Intelligence - Direction du renseignement militaire (France)
EU	European Union
GWB	Act against Restraints of Competition - Gesetz gegen Wettbewerbsbeschränkungen (Germany)
IFG	Freedom of Information Law - Informationsfreiheitsgesetz (Germany)
ISC	Intelligence and Security Committee of Parliament (UK)
NAO	National Audit Office (UK)
NIK	Supreme Audit Office - Najwyższa Izba Kontroli (Poland)
PKGr	Parliamentary Oversight Panel - Parlamentarisches Kontrollgremium (Germany)
SAI	Supreme Audit Institution - Bundesrechnungshof (Germany)
SWW	Military Foreign Intelligence Service - Służba Wywiadu Wojskowego (Poland)
SKW	Military Counterintelligence Service - Służba Kontrwywiadu Wojskowego (Poland)
VertGr	Parliamentary Trust Panel - Vertrauensgremium (Germany)

Introduction

As governments spend billions on procurement every year, the risks posed by poor management, corruption, and waste are significant. To mitigate these risks, democracies subject public procurement processes to a set of fundamental principles, such as transparency, fair competition, and non-discrimination. Nevertheless, specific exceptions exist – for example, procurement in the security and defence sector or in crisis or emergency situations – where, in the interests of national security, these public procurement principles may be limited or circumvented. This is particularly the case for intelligence procurement¹ as intelligence services are more sensitive to protecting procurement-related information that can harm intelligence operations, assets or capacities. Democracies therefore face the challenge of balancing adherence to a set of fundamental guiding principles on the one hand, and meeting national security requirements (protecting sensitive information) on the other. While this issue has been discussed extensively with respect to defence and emergency procurement,² intelligence procurement has received significantly less attention. Recognizing this paradox, states have sought to develop models aimed at balancing these competing demands, in part by subjecting intelligence procurement to specific forms of internal and external oversight. Based on a qualitative comparative analysis, this Thematic Brief will focus on four such models employed in Germany, France, Poland, and the United Kingdom.

The Brief is divided into five sections. It begins by providing an overview of key concepts and definitions related to intelligence procurement. It then outlines regulatory frameworks for intelligence procurement, and describes the conditions under which procurements made by intelligence services may limit or circumvent the application of public procurement principles. It goes on to detail internal and external oversight mechanisms applied to intelligence procurement, before providing recommendations on how to strengthen intelligence procurement systems.

-
- 1 For the purposes of this Brief, intelligence procurement is defined as the purchase by intelligence services of services or goods necessary to carry out statutory tasks.
 - 2 During a disaster or crisis, timely decisions are needed to save lives and protect populations from harm. The Covid-19 pandemic called for public authorities to undertake special procurement measures to secure timely products and services from the private sector with great urgency. For more information on defence and security procurement in general, see: Reid, Elizabeth (contributing ed.). 2021. *Defence and Security Procurement 2021 Edition* (London: Law Business Research Ltd.). Available at: <https://www.twobirds.com/-/media/pdfs/news/articles/2021/global/gtdt-defence-security-procurement-2021.pdf?la=en&hash=3D-365CA80F48DDBCOCC2AABA17464C65D0F89625>.

Key Concepts and Definitions

‘Intelligence procurement’ can be understood as the purchase by intelligence services of services or goods necessary to carry out statutory tasks that, in the interests of state security, may be classified as secret. ‘Public procurement’, on the other hand, can be understood as the purchase by governments and state-owned enterprises – including intelligence services – of goods or services that are subject only to the provisions of public procurement laws and are therefore not classified as secret. Regulations governing such procurements generally take two forms: specific procurement rules and a set of core procurement principles, applicable regardless of the services and goods to which they might apply. In the United Kingdom, for example, these principles include the following:

- **Transparency:** All procurement processes should be transparent, unless there are very good reasons for keeping the process secret;
- **Integrity:** The procurement process should be reliable and available for scrutiny;
- **Value for money:** All procurements should provide maximum value for money;
- **Openness:** Even for sensitive procurements, the process should be visible and understandable to all those bidding for contracts;
- **Fairness:** There should be unbiased decision making when deciding on a contract, and decisions on contracts should compare like with like;
- **Competition:** Unless there are very good reasons not to, all contracts should be subject to competition;
- **Accountability:** All decisions and decision-makers should be accountable for their decisions and scrutinized for their decision making;
- **Integration:** To get the best value for money, contracts should be combined to ensure economies of scale;
- **Legality:** All contracts should conform with national and international legal standards;
- **Responsive to customer needs:** The end customer should be involved in the process;
- **Measures of performance:** All contracts should include ways to measure performance both during and after the contract period.

In Germany, the core principles governing all public procurement processes, which closely resemble those of EU regulations, are outlined in Section 97 of Act against Restraints of Competition (Gesetz gegen Wettbewerbsbeschränkungen, GWB)³ as:

- ensuring fair competition, transparency, economy, and proportionality;
- competing on equal terms, unless legal provisions allow otherwise;
- emphasizing quality, innovation, and regard for social and environmental impact; and
- prioritizing small and medium-sized companies (tenders are supposed to be subdivided into groups and awarded separately according to specified needs).

In addition, public procurement, including that of intelligence services, also generally includes the principle of dividing tenders according to size. According to this general rule, also applicable under EU law⁴, the larger the size of the tender, the more elaborate and complex the tender process, and the higher the level of authority within the organization required to authorize the tender. In the United Kingdom, for example, contracts below GBP 10,000 are normally exempted from a tender process. On the other hand, large capital projects such as buildings, while following the same basic principles, must have project boards made up of clients, procurement professionals, and contract professionals. In Germany, very large-scale procurement processes, such as the building of the new headquarters of German Federal Intelligence Service (Bundesnachrichtendienst, BND) in Berlin, require the involvement of specialized procurement authorities of the federal government.

Regulatory Frameworks for Intelligence Procurement

This section outlines the regulatory frameworks used for intelligence procurement in the United Kingdom, Poland, France, and Germany, respectively.

Procurement by intelligence services is generally regulated by an overarching public procurement law, which provides for some

3 Gesetz gegen Wettbewerbsbeschränkungen (GWB) § 97 Grundsätze der Vergabe. 26 June 2013. Available at: https://www.gesetze-im-internet.de/gwb/_97.html.

4 See Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on Public Procurement. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0024>.

exceptions that accommodate the need to maintain secrecy in the interests of national security. In the United Kingdom, most government procurement is regulated by the 2015 law on Public Contracts. Most procurement for UK intelligence services is dealt with through open websites and the Crown Commercial Service, using a tender process through which companies may bid for contracts. All bids are confidential, and all bidders must demonstrate their capability to carry out the contract. Depending on the thresholds used by the procuring government agency, some tenders may be competitive, while others may be closed. This can be the case, for example, when an intelligence service wishes to use a specific contractor,⁵ or when, for other operational reasons, a tender cannot be made public. All government bodies (including security and intelligence services) have dedicated procurement departments, although low-level procurement (understood as contracts below GBP 10,000) may be conducted by teams within specific departments.

In Poland, the main legal act regulating public procurement is the Public Procurement Act of 11 September 2019, which took effect on 1 January 2021 and replaced the previous Public Procurement Act of 2004. The Public Procurement Act reflects the directives of the European Parliament and the European Council on Public Procurement,⁶ which specify the value of contracts as well as the relevant obligations that apply under public procurement laws. According to Article 13 of the said law, public procurement rules do not apply to the procurement of defence and security articles – or, more specifically, to contracts for intelligence and counter-intelligence activities. Procurements are also regulated by other legal acts, including those relating to the management of public funds (the Public Finance Act of 27 August 2009), the principles of keeping accounting records (the Accounting Act of 29 September 1994), concluding contracts (the Civil Code of 23 April 1964), administrative procedures (the Code of Administrative Procedure of 14 June 1960), unfair competition (the Act on Combating Unfair Competition of 16 April 1993), and money laundering prevention (the Act on the Prevention of Money Laundering and Financing of Terrorism of 1 March 2018).

In France, the intelligence services are legally required to follow the process specified in the Public Procurement Code (Code des Marchés Publics) when making procurements; however, despite this legal

5 Intelligence services may choose to use specific contractors, otherwise referred to as 'trusted suppliers', to provide an additional layer of security as only the service and the supplier are aware of the type of goods being provided. See Section 2.1 for further information.

6 Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on Public Procurement. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0024>.

obligation, intelligence services are authorized to invoke the ‘Secret Défense’ to avoid publishing a call for tenders for specific procurement operations to be financed via the ‘special funds’⁷ allocated by the National Security and Counterterrorism Adviser’s Office, who is a direct subordinate of the President of the Republic. All transfers of funds between intelligence services, as well as the total sum of funds spent on procurements by them, are made public when the government submits its yearly Draft Law on the Settlement of Public Accounts (projet de loi de règlement des comptes) to be voted on and approved.

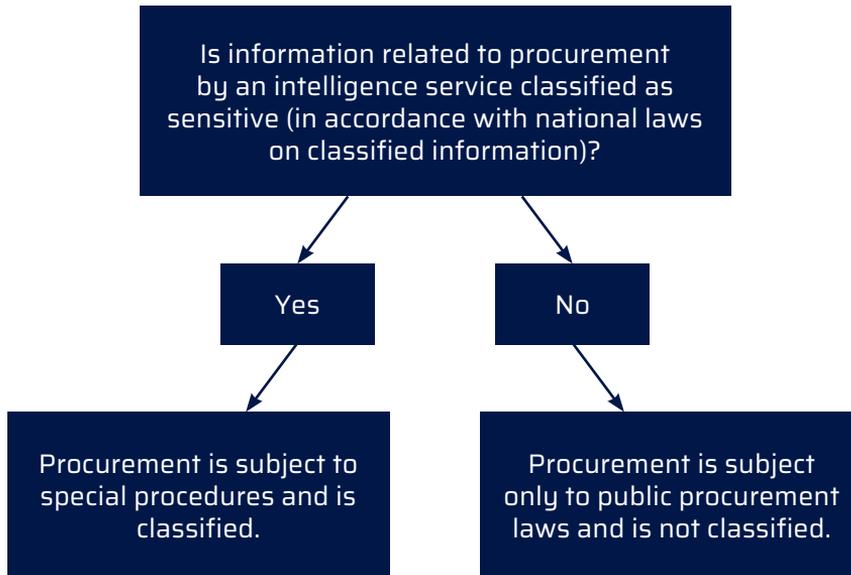
In Germany, the federal intelligence services form part of the federal government. Therefore, all procurement expenditures must be included in the respective budget of the relevant service. In the interests of national security, however, procurement expenditures are structured in such a way as to ensure that the public is not able to see how the funds are allocated. The same authorization and control structure and processes that apply to the budget are applied to procurement-related expenditures. The procurement procedures employed by all authorities and offices of the federal government, including the three German federal intelligence services, are – as far as its key principles are concerned – guided by the same basic legal and regulatory procedures.

1. Intelligence Procurement versus Public Procurement: At What Point Do Special Procedures Apply and Public Procurement Laws Do Not?

As noted above, intelligence procurement is not separate from public procurement procedures; the same overarching procurement principles apply to both. However, if intelligence services determine that sensitive information will be disclosed if a procurement is subject to public procurement laws – regardless of whether such sensitive information concerns the choice of provider, or the services or goods procured – then the procurement in question is subject to special procedures. As a result, procurement procedures, along with their content, become classified information and are therefore subject to a higher level of confidentiality (see Table 1).

7 These so-called ‘special funds’ – also referred to as ‘black budgets’, ‘covert appropriations’, or ‘discretionary funds’ – represent budgets allocated for covert operations and other secret activities that require intelligence services to conceal their efforts. States provide little information on individual amounts and/or the nature of how and when these funds are used. Thus, the extent to which these expenditures are used for intelligence procurement purposes remains unclear.

Table 1. Conditions under which special procedures apply to procurements made by intelligence services



The following section outlines the conditions under which procurement by intelligence services in Germany, France, Poland, and the United Kingdom may be subject to special procedures.

In Germany, intelligence procurement procedures correspond closely to those of other federal government authorities, while procurements that concern sensitive information are subject to special procedures to ensure their confidentiality. Similarly, in France, tenders that aim to fulfill intelligence purposes may be subject to special procedures, but only if they involve sensitive information directly related to intelligence activities.

In Poland, the Public Procurement Act defines the procurement procedures applicable to all units of the public finance sector, including the four constituent intelligence services of the Polish intelligence community with the status of central state administration offices: the Foreign Intelligence Agency (Agencja Wywiadu, AW); the Internal Security Agency (Agencja Bezpieczeństwa Wewnętrznego, ABW); the Military Foreign Intelligence Service (Służba Wywiadu Wojskowego, SWW); and the Military Counterintelligence Service (Służba Kontrwywiadu Wojskowego, SKW). In practice, most procurements – especially the purchase of services and goods typically required for the operation of any state office – are not secret, and are therefore carried out in accordance with the general principles set out in the Public Procurement Act and subject to the supervision and control

of the relevant civil institutions, including the Ministry of Finance and the Public Procurement Office. Nevertheless, Article 12 of the Public Procurement Act guarantees that the purchase of services and goods which are protected according to the Act on the Protection of Classified Information or which must be accompanied by specific security measures, pursuant to separate regulations, are not subject to the Public Procurement Act. In accordance with the Act on the Protection of Classified Information, a secrecy clause may be invoked if the procurement in question contains sensitive information, such as key information about a service's operation that is deemed necessary to protect in the interests of state security. Under such circumstances, however, the procuring service must provide justification for why the procurement contains information of interest to 'state security', and to what extent this interest justifies the need for exclusion from the provisions of the Public Procurement Act. In cases where such justification is provided, the provisions of the Public Procurement Act are not applicable, and the procurement is instead subject to the internal regulations of each service as approved by its head (director). Alternatively, sections of the procurement contract that are deemed sensitive may be subject to secrecy clauses, with the remainder of the contract subject to the provisions of the Public Procurement Act, and therefore not classified. Article 5 of the Act on the Protection of Classified Information of 5 August 2010 describes the type of information that is subject to secrecy clauses.

In the United Kingdom, procurements by intelligence services, as well as the Ministry of Defence, are in general not subject to the provisions of the Public Contracts Regulations 2015. They must, nevertheless, adhere to the general principles outlined above.⁸ The 2011 Defence and Public Contracts Regulations and exemptions to the 2015 regulations permit the services to hide their processes from the public while complying with all of the basic principles.

2. Intelligence Procurement: Features, Exemptions, and Special Procedures

The section above has illustrated that, in the cases of France, Poland, Germany, and the United Kingdom, regulatory systems provide a means through which procurements by intelligence services may be subject to special procedures, and therefore exempt from certain public procurement rules. As a result, procurement by intelligence services is distinct from standard procurement procedures in terms of the process through which providers and foreign contractors are selected; the degree of competition and transparency in the tender

⁸ These principles include transparency, integrity, economy, openness, fairness, competition, accountability, integration, legality, responsiveness to customer needs, and measures of performance.

process; the management structure for procurements; and, to a lesser degree, inter-agency cooperation. These factors will be addressed below.

2.1 Selection of specific providers and foreign contractors

Classified information concerning procurements by intelligence services that are subject to special procedures needs to be protected. For this reason, the selection of specific providers and foreign contractors calls for enhanced security measures, such as the requirement that such vendors be subject to security clearances, and the imposition of additional security measures for the use of foreign contractors.

Security clearance

In general, security clearance can be understood as a status granted to an individual or entity to allow them access to classified information. In the context of intelligence procurement, potential vendors may be required to hold security clearances before their services can be used. In Germany, this process is standardized and includes several levels of potential clearance.⁹ The level of security clearance required depends on the level of sensitivity of the procurement process in which the potential vendor may be involved. A specific requirement for vendors was introduced in 2014: the so-called ‘no-spy clause’.¹⁰ This clause requires all vendors involved in security-related tender processes to sign a declaration guaranteeing that they will prevent the transfer of sensitive data to foreign intelligence services.¹¹

In the United Kingdom, intelligence services can only use the services of vendors who have been officially registered; namely, those who hold security clearances and who have been subject to a process of due diligence. The names of registered vendors – referred to as ‘List X’ companies – appear on a registration list held by the individual service or the Ministry of Defence. In theory, any company can apply for ‘List X’ status. If they pass the security clearance and due diligence process, they are granted special permission to hold government secrets and confidential information, and added to ‘List X’. Alternatively, the intelligence service can choose to use only so-called ‘trusted suppliers’

9 The higher the level of clearance, the more complex and intensive the investigation of the background of the company and its employees.

10 For more information, see: German Federal Ministry of the Interior (Bundesministerium des Innern). 30 April 2014. Handreichung zum Erlass an das Beschaffungssamt des BMI (BeschA), 04 – 11032/23#14. Available at: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2014/no-spy-erlass.pdf;jsessionid=95FC33745F4EC66E541F20EEAF160DE0.1_cid373?_blob=publicationFile&v=1.

11 Interestingly, this requirement also relates to potential foreign, including EU, vendors. For more information, see *ibid*.

when declaring the end user. Using ‘trusted suppliers’ provides an additional layer of security as only the service and the supplier are aware of the type of goods being provided. These suppliers must have security clearance and any relationships with existing or former staff of intelligence services must be declared. In addition, the suppliers must declare any relationship with foreign entities, including supplying similar services to an overseas government, any investment in the company by overseas companies, and any overseas ownership. Furthermore, the financial situation of companies is closely scrutinized to ensure their liquidity and prevent vulnerability to pressure from hostile actors. In addition to the above, any staff selected to work on the specific contract must undergo additional security clearance procedures. For national security reasons, non-UK nationals are normally excluded from such contracts, primarily because it is difficult to carry out the vetting of foreign citizens.

The need for security clearance for potential vendors, as well as the level of security clearance required, may depend on the level of sensitivity of procurement material. In Germany, the general administrative rules are increasingly applied to the procurement of less sensitive materials. A case in point concerns a public tender announcement for magnetic locks for doors at the new BND headquarters in Berlin.¹² While the provisions of the public procurement tender did not limit the type of company that was able to apply, they did provide several restrictions to ensure the necessary level of confidentiality, including the following: the company must have been located in Germany for at least one year; the company could not be connected (currently or previously) in any way to countries included on the government’s list of states that present an increased security risk;¹³ and the company must have signed a specific set of documents related to the confidentiality of information.

For intelligence procurements concerning highly sensitive information, the issuing of security clearances is subject to additional measures to ensure the protection of such information. For example, in Germany, a subcategory of procurement relates to technologies whose development is considered extremely sensitive and that are therefore classified to the highest level. For these technologies, in-house development is the preferred method.¹⁴ This may also involve

12 For more information, see Bauportal Deutschland: https://www.bauportal-deutschland.de/oeffentliche_ausschreibung_vobvol_details_10115_Berlin_Elektromechanische_Schliesszylinder_610556.html.

13 The list is compiled by the federal government and indicates states that are considered an enhanced security threat.

14 In-house development refers to the process through which intelligence services rely exclusively on their own staff to develop products. In Germany, intelligence services may also involve other centralized state agencies such as the Central Office for Information Technology in the Security Sector (ZITis), a technology

cooperation with allied foreign intelligence services.¹⁵

Foreign contractors

Under special procedures, intelligence services may be allowed to impose additional requirements on potential vendors, in particular foreign contractors. In Germany, for example, all foreign contractors must be registered in the country; the security clearance process for such vendors is therefore significantly more complex and resource intensive. As a result, the engagement of foreign vendors remains the exception rather than the rule. In France, intelligence services are allowed to contract foreign contractors for specific purposes when there is no domestic solution or product available. A case in point concerns the General Directorate of Internal Security's (Direction générale de la sécurité intérieure, DGSI) use of the services of the American company Palantir, which specializes in big data analysis. British intelligence services rarely use foreign contractors, except through UK third parties who supply goods. When foreign suppliers are used, procurement will generally be facilitated by a government procurement agency to ensure that the end user (in this case, the individual service) will not be known. However, the use of foreign contractors remains limited; their services are only engaged when specific expertise is needed, often with the cooperation of overseas liaison services. In Poland, the rules concerning the use of foreign contractors are less stringent. In general, foreign contractors may apply for a contract if it is executed in the form of an open tender procedure, and if they possess an industrial security certificate. In the case of direct agreement contracts, the service may also contract the services of a foreign vendor.

2.2 Limiting competition and transparency

The ability of intelligence services to subject procurements to special procedures limits the principle of competitiveness. In some cases, intelligence services may be exempted from calling for tenders altogether. For example, even if compelled by law to go through the Public Procurement Code process, French intelligence services are authorized to invoke the 'secret défense' to avoid publishing a call for tenders for specific procurement operations financed through the special funds allocated by the National Security and Counterterrorism Adviser's office.

service provider for German security and intelligence services in the cyber sector. For more information, see: https://www.zitis.bund.de/DE/ZITIS/Aufgaben/aufgaben_node.html.

15 As documented by the recent revelation of the so-called 'Operation Rubicon'. See for example: Theveßen, Elmar, Peter F. Müller, and Ulrich Stoll. 11 February 2020. 'Operation Rubikon: Wie BND und CIA die Welt belauschten'. Available at: <https://www.zdf.de/politik/frontal-21/operation-rubikon-100.html>).

In Poland, intelligence procurement may be carried out through the so-called 'direct agreement' (single source) contract mode, otherwise referred to as a 'non-competitive procedure'. Under this model, the contracting authority negotiates the terms of the contract with the contractor of its choice. In Poland, the 'direct agreement' intelligence procurement procedure applies regardless of the value of the contract, which distinguishes it from public procurements contracts, where contracts valued at PLN 130,000 (approx. EUR 30,000) or more are subject to the general provisions of the Public Procurement Act and therefore carried out through an open tender procedure. Derogations from this rule are strictly defined the same law. The activities of each of the services, property management, and the purchase of services and goods are regulated by service-specific laws, referred to as 'Acts of Agencies'.¹⁶

In Germany, intelligence procurement under Section 146 of the GWB allows for a closed tender process.¹⁷ Crucially, however, the provisions contained within these regulations do not define the state authorities that may conduct procurements through closed processes, but rather consider the aim of the tender as the key criterion.

2.3 Decentralized management

Intelligence services have adopted decentralized management processes and structures for intelligence procurements. The purpose of this decentralization is threefold: to limit the number of people within a chain of command who have access to confidential information; to provide flexibility with respect to the procurement of operational requirements; and to reduce the risk of abuse by ensuring that no single individual is involved in the proposal, approval, and decision-making process. This model is used in Poland and the United Kingdom. In the former, the head of each service has the prerogative to determine their internal regulations for intelligence procurements. Contracts containing sensitive information that cannot be governed by the rules on public finance, accounting, and public procurement are financed by so-called 'special funds' set up for this purpose, which are a secret part of each service's budget. The guidelines for creating and managing this fund are defined by internal regulations adopted by the heads of each service. In the case of military services, the orders issued by their chiefs must be approved by the minister of defence.

In the United Kingdom, both national procurement bodies and the service's individual procurement department will normally oversee

16 These include the ABW and AW Act of 24 May 2002 and, for military services, the SKW and SWW Act of 9 June 2006.

17 For more information, see: GWB, § 146. Available at: https://www.gesetze-im-internet.de/gwb/_146.html. See also: GWB § 145 and § 107; and Directive 2009/81/EC of the European Parliament and Council of 13 July 2009, para. 13 (b).

procurement processes. Their responsibilities finish once the contract is signed, after which the contracts department and the client usually monitor the fulfilment of the contract. To protect national security, operational budgets are delegated to team managers, so they can ensure that expenditure does not follow an obvious pattern. For example, if all operational staff were required to use a single airline or hotel chain, their identities might be easily discoverable by foreign services or hostile actors.

While team managers have broad discretion regarding low-level purchases, to reduce the risk of corruption they are subject to limits on single-item purchases and on the types of expenditure. Low-level purchases, such as airline tickets, must be limited to a certain amount and made in the name of the individual concerned rather than that of the service. As a result, the service provider is unaware that they are providing tickets for intelligence operatives. To ensure control of low-level purchases, team managers are accountable to an independent departmental finance officer and must justify their expenditure. No manager is authorised to make all the purchases on behalf of a particular service, nor may they use one service provider exclusively. Furthermore, if members of intelligence services are connected to service providers, they must declare this; failure to do so results in dismissal.

2.4 Inter-agency cooperation

Intelligence services also tend to cooperate with each other with respect to procurement. In the United Kingdom, for example, intelligence services and the Ministry of Defence are increasing the use of joint procurements, partly owing to the advantages of increased buying power, but also owing to the growing need for interoperability (that is, the ability to work together using the same type of equipment). Furthermore, intelligence services may outsource the procurement of non-sensitive materials (such as stationary) to another government department.

Similarly, for operational, technical, or organizational needs, French intelligence services regularly transfer funds between each other or share expenses. In general, these funds are used for common technical programmes. For example, as the primary SIGINT (Signal Intelligence) service of the French intelligence community, the General Directorate for External Security (Direction générale de la sécurité extérieure, DGSE) regularly receives funds from the initial budgetary allocations of the DGSI and the Directorate of Military Intelligence (Direction du renseignement militaire, DRM) to assist in its development of complex and long-lasting technical solutions and equipment.

3. Oversight of Intelligence Procurement

The following section will provide an overview of the types of internal and external oversight measures applied to intelligence procurement, which are somewhat limited and primarily concern the role of audit offices, the parliament, and, to a lesser degree, public oversight.

3.1 Internal oversight

Intelligence services exercise internal oversight over procurements through a complex set of mechanisms and measures. These mechanisms and measures vary from country to country. In France, for example, the Directorate of Administration of the DGSE oversees and controls all the expenses made by the different directorates, including those from special funds. The Director General is also assisted by a legal adviser, who is a full member of their personal cabinet and required to provide advice on any contract signed by the service.

In the United Kingdom, each service has its own regulations and processes that govern procurements. Internally, all expenditure is monitored through the service's management chain, with every manager expected to undergo financial training. In addition, procurement and expenditure is closely monitored by the finance departments of the services. If staff abuse the procurement process, they are liable to prosecution under the 2007 Theft Act. In such cases, investigations are independent and carried out by the police.

In Poland, the head of each service is responsible for developing a system for internal oversight. For this purpose, under the Public Finance Act, each head is obliged to create a management control system consisting of institutional elements, which include a control section in the finance office, control sections in organizational units, and an independent internal audit unit. Direct supervision over procurements is exercised by the chief accountant and the appointed authorized deputy head of the service. The chief accountant of each service also holds the position of director of their respective finance office. Each finance office is composed of specialized sections responsible for financial control, which are responsible for controlling the expenditures of organizational units authorized to issue contracts with service providers. In addition, the internal audit unit is tasked with reviewing procurement processes and identifying irregularities. In contrast to financial units, the internal audit office has the right to access operational documentation. In the case of military services, relevant internal regulations are determined by the Ministry of National Defence.

3.2 External oversight

In addition to internal oversight, each country has a general institutional

framework for exercising external oversight over intelligence procurements, which varies depending on the ministry to which the service is subordinated. For example, if intelligence services use special funds in France, they are required to liaise with the National Security and Counterterrorism Adviser to oversee their expenditure. Furthermore, the use of special funds is monitored and controlled by the Special Funds Verification Committee (Commission de Vérification des Fonds Spéciaux, CVFS), an external oversight body composed of two members of parliament and two senators. The CVFS may access any administrative document or invoice concerning special funds but is not authorized to access information regarding operations or sources linked to such expenses. The different ministries to which the intelligence services are subordinated are also obliged to submit yearly reports to the government, the contents of which include certain information on procurements by intelligence services. These reports are then compiled into the Draft Law on the Settlement of Public Accounts and subsequently discussed, approved, and adopted by the parliament.

In Poland, the external oversight of budget expenditure is exercised by the Ministry of Finance. Agencies report on budget implementation on a monthly basis, based on the rules applicable to all public bodies. The Prime Minister enjoys the right to ex-post control (audit) of individual aspects of the service's activities, including classified activities, pursuant to the Act on Control in Government Administration of 15 July 2011. Accordingly, he or she may order the internal audit unit within the Chancellery of the Prime Minister to audit selected procurements. Nevertheless, such audit units do not have the right to access all documentation, in part due to the restrictions imposed by the provisions of the ABW and AW Act of 24 May 2002 and, for military services, the SKW and SWW Act of 9 June 2006.

The Prime Minister may appoint a Minister for Coordination of Intelligence and Security Services, and delegate to them his or her powers related to the control and oversight over the management of public funds by the services subordinate to him or her. Such powers include the conducting of ad hoc ex-post audits concerning selected contracts or particular categories of contracts. The Minister of National Defence has oversight powers over Polish military services, which are exercised through ongoing oversight of the implementation of the budget of each service, and the right to carry out ad hoc ex-post controls by ministerial audit units subordinate to the Ministry of National Defence.

Audit office

While the previous section outlined internal oversight systems, referencing in particular the role of internal audit offices, most countries also have a designated independent audit office, which is

responsible for monitoring intelligence procurements. For example, the UK intelligence services' finance departments are monitored by the National Audit Office (NAO), which has staff within the services. The NAO are independent and have the power to review all accounts to ensure the services are exercising proper financial and procurement management. Furthermore, certain expenditures by intelligence services are included in the annual financial statement of the security and intelligence services, but only at a general level.

The Polish Supreme Audit Office (Najwyższa Izba Kontroli, NIK) has the power to oversee and control intelligence procurements. The NIK is also able to request financial documentation from each service, including those related to the execution of intelligence contracts. While the NIK has the right to view full accounting documentation related to all types of orders, it may not access documents or information concerning the forms and methods of work, nor data that may reveal the identity of officers and persons providing covert cooperation (information sources).

In Germany, in addition to internal audits conducted by the administrative departments within each of the three services, the procurement processes of the services - as for all federal government authorities - are subject to regular audits by the Supreme Audit Institution (Bundesrechnungshof, SAI). The SAI reports to the federal parliament - in this case the Parliamentary Trust Panel (Vertrauensgremium, VertGr), which in turn informs the Parliamentary Control Panel (Parlamentarisches Kontrollgremium, PKGr). This ensures the independence of audit procurement processes.

Parliamentary oversight

Parliamentary oversight over intelligence procurement is most often exercised by designated parliamentary committees. Some countries have dedicated committees for intelligence services, while others have committees responsible for oversight over the broader security and defence sector. In the United Kingdom, which uses the former model, the Intelligence and Security Committee of Parliament (ISC) carries out independent scrutiny of intelligence expenditure and procurement. While these discussions are rarely carried out in public, the ISC do occasionally publish reports, such as the report into the procurement of the National Cyber Security Centre headquarters.

The German structure maintains in general the same parliamentary oversight and control mechanisms that it employs for other government authorities. The VertGr, the subcommittee of the budget committee of the federal parliament, and the PKGr are central to authorization and parliamentary oversight processes. These bodies conduct their deliberations confidentially but report to the parliament (plenary). For 'regular' procurement processes, the VertGr is the lead mechanism

that authorizes expenditure by authorizing the various budget lines. When procurement processes are particularly large, the PKGr is also involved. All parties represented in the federal parliament are also represented in both intelligence oversight bodies.¹⁸ Similar to its function within the budget cycle for the intelligence services, the VertGr also has a mandate to monitor and control the services' procurement processes, and reports regularly to the PKGr and, in a generalized manner, to the members of the federal parliament.¹⁹ Similarly, the PKGr monitors important procurement projects of the services and exercises oversight through its ability to request information from the services and to interview officials from the services.²⁰ Additional parliamentary oversight is ensured through the right of each member of the federal parliament to ask specific questions to the federal government, including questions related to the intelligence services' procurement projects,²¹ and through the establishment of special investigative committees (Untersuchungsausschüsse), established upon the request of at least a quarter of all members of parliament. If a special investigative committee deliberates on issues that are

-
- 18 In the current VertGr, however, only one party – the Alternative für Deutschland (AfD) – is not represented as it did not manage to get the required parliamentary votes, which are necessary to get a member appointed to the subcommittee. For more information, see: Deutscher Bundestag. 10 September 2020. 'Keine Mehrheit für AfD-Kandidaten zur Besetzung von Gremien'. Available at: <https://www.bundestag.de/dokumente/textarchiv/2020/kw37-de-wahlen1-790836>; see also Bundeshaushaltsordnung (BHO) § 10a Geheimhaltungsbedürftige Angelegenheiten. 19 August 1969. Available at: https://www.gesetze-im-internet.de/bho/_10a.html.
- 19 See for example: Bundestag. 22 July 2013. 'Vertrauensgremium legt Bericht zum BND-Neubau vor – mindestens 1,4 Milliarden statt geplante 720 Millionen Euro'. Available at: <https://www.vergabeblog.de/2013-07-22/1457-milliarden-euro-ab-sehbare-gesamtkosten-fur-verlagerung-der-bnd-zentrale-und-verkleinerung-des-alten-standortes/>. For the original VertGr report, see: Deutscher Bundestag. 5 July 2013. 'Unterrichtung durch das Vertrauensgremium gemäß § 10a Absatz 2 der Bundeshaushaltsordnung. Bericht über die Tätigkeit des Vertrauensgremiums im Zeitraum Januar 2012 bis Juni 2013'. Available at: <http://dip21.bundestag.de/dip21/btd/17/143/1714344.pdf>.
- 20 The various mechanisms through which the PKGr conducts its work are outlined in the PKGr law, see: Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (Kontrollgremiumgesetz - PKGrG). 29 July 2009. Available at: <https://www.gesetze-im-internet.de/pkgrg/BJNR234610009.html>.
- 21 However, parts of the federal government's response to the question of the respective parliamentarian may be restricted if they disclose information that is classified. In these cases, the federal government must justify in detail why the response is incomplete. In critical cases, this justification can be contested in a court. For more information, see: Deutscher Bundestag, Parlamentarische Informationsrechte über den Haushalt des Bundesamtes für Verfassungsschutz und des Bundesnachrichtendienstes. 3 March 2014. page 6f. Available at: <https://www.bundestag.de/resource/blob/412544/9eb628d6634d031c4214f16b-c210f232/WD-3-047-14-pdf-data.pdf>

classified, its sessions will be conducted without the participation of the public.²²

Public oversight

Public oversight concerns the role of civil society and the media in overseeing the security and defence sector. Given the nature of intelligence activities, such oversight is rather limited. In most states, including the United Kingdom and Germany, civil society does not have a formal role in overseeing intelligence procurement. In Germany, however, since large-scale intelligence procurements involve public tender processes, certain information is sometimes reported in the German media. This enables civil society organizations, such as the Bund der Steuerzahler (Association of Taxpayers), to have an indirect influence on procurement processes through public criticism and advocacy and to keep the public informed.²³

Furthermore, the federal government is obligated to keep the public informed about its activities and spending. All citizens have the right to request information from any government authority, including the intelligence services, in accordance with the Freedom of Information Law (Informationsfreiheitsgesetz, IFG).²⁴ While the government may restrict the content of the information it releases upon a citizen's request,²⁵ it must justify the reasons for doing so. Such justifications may also be contested in court.

In France, the regulatory framework in place for intelligence procurement provides for public access to information related to technical and logistical equipment and supplies, human resources, and real estate matters. As with any other administration, the intelligence services are legally required to generate their procurement through the Public Procurement Code (Code des Marchés Publics) and are therefore compelled to provide information on their technical, logistical, realty properties, and personal needs. Transfers and the expenditure of funds for intelligence procurement are made public

22 Deutscher Bundestag. Untersuchungsausschüsse. 27 March 2009. Available at: <https://www.bundestag.de/resource/blob/190568/ce3840e6f7db-fe7052aa62debf812326/untersuchungsausschuesse-data.pdf>.

23 See, for example, documentation and criticism of the Bund der Steuerzahler concerning the building of the BND headquarters in its annual publication 'Schwarzbuch', which documents wasteful government spending: Bund der Steuerzahler, Das Schwarzbuch. Die öffentliche Verschwendung 2019/20. p. 96. Available at: https://steuerzahler.de/fileadmin/user_upload/Schwarzbuch2019_web.pdf

24 Gesetz zur Regelung des Zugangs zu Informationen des Bundes (Informationsfreiheitsgesetz, IFG). 5 September 2005. Available at: <https://www.gesetze-im-internet.de/ifg/>

25 Particularly when, for example, the information may negatively affect Germany's security, see *Ibid.* § 3. Available at: https://www.gesetze-im-internet.de/ifg/_3.html.

after the government submits its yearly Draft Law on the Settlement of Public Accounts (projet de loi de règlement des comptes) to be voted on and approved. This document contains information on the expenditure of each service during the preceding fiscal year, including the total sum of special funds spent. Civil society are therefore able to monitor intelligence procurement to a certain extent, exemplified by the existence of several blogs specializing in defence and intelligence matters, such as 'Zone d'Intérêt' and 'Bug Brother', as well as the newspaper 'Le Canard enchaîné' and the daily confidential letter 'Intelligence Online'.

Recommendations

Based on the above analysis, the following recommendations can be made:

- **Ensure maximum procurement transparency:** Even when subject to special procedures, intelligence procurement processes should be transparent to the maximum extent permitted by operational needs, and understood by all staff, auditors, and contractors involved. The provisions governing intelligence procurement should be clear and, with the exception of internal intelligence procurement regulations, unclassified. Emphasis should be placed on clearly defining the conditions under which procurements made by intelligence services may be excluded from general provisions on public procurement. The criteria to assess when such conditions are met should be unambiguous and precise so as to avoid unjustified and unreasonable (arbitrary) discretion.
- **Decentralize procurement management:** Allowing operational teams within intelligence services certain discretion over operational expenditure helps to ensure that it does not follow an obvious pattern, and therefore prevents foreign agencies or hostile actors from discovering the identities of intelligence operatives or the nature of their operations. Nevertheless, to reduce the risk of abuse, responsibility for expenditure should be spread widely among staff to ensure that no single individual is in charge of the process. Alternatively, the separation of the client/customer from the procurement process and the separation of the procurement process from contract management may also be considered. In this way, no one person or group of individuals has control over more than one aspect of the procurement process.
- **Ensure the fair and competitive selection of vendors:** The criteria used for the selection of specific providers should be proportionate to the need to protect national security, and should

not unduly discriminate or arbitrarily limit the involvement of potential vendors. In the case of direct agreements, in the absence of a public call for tenders, the criteria for the selection of specific vendors should be clear and follow the principles of public procurement. The internal procurement regulations within each service should also reflect these principles.

- **Ensure oversight can be conducted effectively:** Internal provisions for intelligence procurement should be subject to external scrutiny and require external executive approval before being adopted by the service. Such provisions should clearly define and indicate the responsibilities of specific persons for decisions on applications for an exemption from the general provisions for procurement procedures, along with the factual justification for these decisions. Furthermore, external entities authorized to conduct audits should have a strong legal mandate, preferably statutory, and proper authority to access information necessary to determine the material truth, including the right to obtain testimonies from officers under oath. The limits of these powers, such as access to information concerning operational activities, should be defined precisely and unambiguously.
- **Develop an institutional structure for monitoring procurement processes:** The placement of finance officers in departments to monitor expenditure ensures that operational expenditure provides value for money and avoids abuse of expenditures. This is further strengthened by ensuring independent financial management, such as through the system used in the United Kingdom, in which officers from the NAO are embedded within the services.

DCAF Geneva Centre
for Security Sector
Governance

DCAF Geneva Headquarters

P.O.Box 1360
CH-1211 Geneva 1
Switzerland

✉ info@dcaf.ch

☎ +41 (0) 22 730 9400

www.dcaf.ch

🐦 [@DCAF_Geneva](https://twitter.com/DCAF_Geneva)