Home Office

Guide to the National Security Act 2023 for Security Professionals

January 2025

This publication is available at National Security Act 2023 - GOV.UK (www.gov.uk)

Contents

Do you know who you're working for? 2

What are state threats? 3

- Dissidents 3
- Sensitive government, research or business information 3
- Critical infrastructure 3

The National Security Act 2023 4

- The Foreign Influence Registration Scheme (FIRS) 5

Do you know who you're working for? 6

- Which states should I be worried about? 6
- How will I know that I have been approached by a state actor? What signs should I look for? How do I verify the authenticity of a potential client? 6
- What should I do if I think I've been approached by a state? Who should I report it to? What action should I take? 7
- What if I realise halfway through a contract that I have been working for a foreign power? What will the consequences be for me or/ my business if I report it? 7

Further resources and guidance 8

Annex A – Example scenarios 9

- Example scenario A 9
- Example scenario B 9
- Example scenario C 9

Do you know who you're working for?

The services you offer as a security professional may be attractive to state actors looking to undertake malign activity in the UK and you may be at risk of committing an offence under new legislation.

We need your help to harden our society against state threats.

- **Be vigilant:** have an awareness of state threats activity and the signs you can look out for.
- **Due diligence:** you should establish who your client is and whether they are part of a foreign power.
- **Spread the word:** tell those who work across your sector about the new legislation and how to comply.

What are state threats?

State threats are overt or covert actions by foreign governments which fall short of direct armed conflict but go beyond peaceful diplomacy and expected statecraft to harm or threaten the safety or interests of the UK.

State threats activity can take a variety of forms; broadly it describes activity that damages the UK or its interests, such as causing damage to assets and infrastructure (sabotage) or stealing sensitive information (espionage). It also covers activities intended to undermine our values and freedoms, such as manipulating public discourse or threatening political dissidents in the UK, ranging from harassment to physical threats.

UK security professionals are at risk of being approached by certain states to undertake activities in the UK due to their access to valuable sources of information. You may be asked to gather information from a range of sources to support a state actor's strategic aims.

Dissidents

State actors look to gather information on organisations and/or individuals whose work or stance is critical of that state or who are otherwise determined to pose a risk to regime stability. Activity could include gathering information on their pattern of life, associates and vulnerabilities, which could assist in the undertaking of intimidation or even serious physical threats, up to and including assassinations.

Sensitive government, research or business information

State actors seek protected or sensitive information from UK national and devolved governments, strategic industries, academia and research institutions to gain an advantage. State actors could seek to exploit this information to improve their own technological or military capabilities or to establish non-public political or diplomatic insights.

Critical infrastructure

State actors target our assets and services in order to harm the UK today, or to identify potential vulnerabilities, including single points of failure, to exploit in the future. Tactics can include collecting information about design, configuration and operation for technical access, or to gain control of supply chains through investment or monopolisation.

You can find some example scenarios of how this activity might manifest within the security sector at Annex A.

The National Security Act 2023

Conducting any of the above activities on behalf of a state could constitute an offence under the National Security Act 2023.

Parts 1 to 3 of the National Security Act 2023 were brought into force on 20th December 2023 to provide the security services and law enforcement agencies with the tools they need to disrupt the full range of state threats. The threat is ever evolving, and we need to stay one step ahead. The Act allows us to keep pace with the changing threat and will make the UK an even harder target for those states which seek to conduct hostile acts.

You may be at risk of committing an offence if the work you are undertaking could **assist a foreign power in carrying out activities against the UK**. For example, you may face prosecution if:

- you are working for a foreign intelligence service, including second parties that are contracted by these organisations. This includes providing information, access to information, goods, services, or financial benefits.
- you accept or agree to accept a material benefit (including financial benefits or information) that originally comes from a foreign intelligence service. The benefit could be received indirectly through an intermediary; you may face prosecution if you ought reasonably to have known that the benefit was provided by or on behalf of a foreign intelligence service.
- you carry out foreign interference activity for, or on behalf of, or intended to benefit a foreign power. Foreign interference is misinformation or disinformation intended to sow discord, manipulate public discourse, discredit or harm the political system or the provision of services to the public, interfere with the development of policy, interfere with the fundamental rights of others and undermine the safety or interests of the UK.
- you obtain, copy, record, retain, disclose, or provide access to protected information and your conduct, or course of conduct of which it forms a part, is carried out for or on behalf of a foreign power.
- you, without authorisation, obtain, copy, record, retain, disclose, or provide access to a trade secret (e.g. confidential information of commercial value) and your conduct, or course of conduct of which it forms a part, is carried out for or on behalf of a foreign power.

These offences, like most in Part 1 of the National Security Act 2023, apply whether the person's conduct takes place in the UK or elsewhere.

The Foreign Influence Registration Scheme (FIRS)

The Act also introduces a new Foreign Influence Registration Scheme (FIRS), which will bring greater transparency of foreign power influence in UK democracy and politics and provides greater reassurance around the activities of foreign powers who pose the greatest risk to UK safety and interests.

FIRS will require the registration of arrangements to carry out political influence activities in the UK at the direction of a foreign power. The enhanced tier of FIRS gives the Secretary of State the power to require registration of a broader range of activities for specified countries, parts of countries or foreign government-controlled entities where this is necessary to protect the safety or interests of the UK.

In line with similar international schemes, registrations can be made through an online portal. Registration of an arrangement does not, in itself, mean that it is illegitimate or illegal. There is no requirement for activity registered with FIRS to cease.

Detailed guidance will be provided ahead of the scheme's requirements coming into force.

Do you know who you're working for?

Below we have provided some guidance on what actions you can take to protect yourselves against committing an offence under the National Security Act 2023.

Which states should I be worried about?

The heads of MI5 and SIS have spoken about the growing threat from states, with the Director General of MI5 previously confirming that the threat predominantly comes from Russia, Iran and China.

However, the legislation is actor agnostic and you may be liable if you are working for any foreign power where the activity is damaging to the safety or interests of the UK.

You should consider how your work complies with the law whichever country you believe a task might be coming from and register with FIRS where appropriate once the scheme comes into effect.

How will I know that I have been approached by a state actor? What signs should I look for? How do I verify the authenticity of a potential client?

The direct involvement of a state may not be immediately obvious. Many state actors operate covertly, making it harder to discover their intentions or involvement. Some states target the UK through intermediaries.

Some state actors can compel their citizens to work with intelligence agencies, willingly or not, to meet state requirements.

You should take all reasonable precautions you feel appropriate to reassure yourself that you are not undertaking damaging activity for a foreign power. This guidance is designed to aid you in reducing risk to yourself and your business and will not be able to eliminate it altogether. Some questions you could ask yourself include:

1. Is your client based overseas and are they likely to be working for a state? E.g. public sector or arm's length body?

2. Has your client failed to provide you with sufficient information as to their identity or organisation when requested?

3. Could the activity they are asking you to carry out fall under any of the behaviours outlined above? (e.g. gathering sensitive information on an individual or national infrastructure)

If you answer ‘yes’ to one or more of these questions, you should strongly consider whether you take on the contract for that client.

What should I do if I think I’ve been approached by a state? Who should I report it to? What action should I take?

If your due diligence on a client and their requirements leads you to suspect the involvement of a state, report in confidence by calling the Anti-Terrorism Hotline on 0800 789 321 or online at gov.uk/ACT. Counter Terrorism Policing are responsible for responding to threats from hostile states as well as terrorism.

If you have been approached to undertake activity that you suspect may lead to threat to life (e.g. you have been asked to gather information on pattern of life and locations of a dissident for instance), you should report it to 999 or 101.

Further information on what you should do if you are unsure whether you need to register your activity under FIRS will be published ahead of the scheme coming into effect.

What if I realise halfway through a contract that I have been working for a foreign power? What will the consequences be for me or/ my business if I report it?

You should report a client at any point in a business relationship when you become suspicious of their intent or provenance; however, the act of reporting does not negate your responsibilities under the law. We encourage due diligence before taking on a new client or contract.

Further resources and guidance

The MI5 website sets out in more detail the risks that state threats pose and the kinds of behaviour they are countering day to day. There is also a news section which includes the latest published updates on the threat, such as the head of MI5's annual threat speech.

Gov.uk has detailed factsheets on the legislation, including on the Foreign Influence Registration Scheme. If you have questions or are unclear on whether this legislation applies to your business activities, you should consult the official guidance in the first instance.

National Protective Security Authority's threat page also provides an overview on state threats to businesses. They offer guidance on how to protect your business from hostile activity. This may assist organisations seeking to review their risk assessments or update their security policies.

Annex A – Example scenarios

Below are some non-exhaustive examples of state threat activity relevant to the security profession:

Example scenario A

Person A is approached to collect personal information on an individual of interest's home address, pattern of life and associates. The individual is a well-known dissident from another state.

Person A is aware of reporting in the press which implicates the intelligence services from the person of interest's country of origin in the surveillance of dissidents, including the individual in question. The client refuses to explain why they need the information. Person A is aware that the information is of such nature that it would be valuable to a foreign intelligence service that was seeking to harm the dissident. Person A discloses the information collected on the individual to the client. Person A knows, or at least ought reasonably to know, that the provision of this information could assist a foreign intelligence service in carrying out UK-related activity.

Example scenario B

Person A provides close protection for the owner of a prominent defence contractor. When an individual (Person B) approaches them and offers a sizeable payment to report back conversations they have heard regarding current contracts their client is working on, A accepts and begins sharing sensitive information.

B claims to work for a commercial competitor but A cannot find any details of the company online and forms the view that B is working on behalf of a foreign state. A knows, or at least ought reasonably to know, that the provision of this sensitive information could be providing a strategic advantage to another state on UK defence activity.

Example scenario C

Business A was offered a contract to undertake security consultancy on the construction, in the UK, of a building by a foreign government. During that contract, Business A was asked to disclose measures used to protected UK government buildings. Business A provides this UK government information to the foreign government, committing an offence under the National Security Act 2023.