Code of practice for companies that provide technical surveillance counter-measures services

NCP 110.3

April 2019

National Security Inspectorate
Sentinel House,
5 Reform Road
Maidenhead
SL6 8BY
Website: nsi.org.uk

This code of practice is to be read in conjunction with the NSI Regulations and the relevant NSI Gold or Silver approval criteria.

No company shall hold out or claim that it adheres to this Code, save by virtue of holding NSI approval, or having obtained the written permission of NSI.

Revision history		
Version	**Date**	**Summary of changes**
3	Apr 2019	Updates to Section 3 Terms and Conditions; Section 4.1 Structure; Section 4.5 Document Control and Records; Section 5.2.3 Terms and Conditions for permanent staff.

Contents

In this document, material (such as guidelines, information, recommendations, advice) that does not form a mandatory requirement of this code of practice is shown in italics

1 Introduction

In the absence of any specific British Standard or other publicly available code of practice, The National Security Inspectorate may approve companies to the principles of ISO 9001 and, for 'service' companies, the general recommendations given in BS 7499, but with additional requirements for basic job training and specialist training, where considered appropriate. In certain cases, it becomes apparent that there is a particular need to specify requirements for a company providing specific services and a dedicated code of practice is then produced.

This NSI Code of Practice has been developed to provide guidelines for the operation and management of a company providing technical surveillance counter-measures services. This Code acts both as a means of advising such companies of the NSI approval criteria and to form a consistent basis for inspecting all aspects of these services.

No company shall hold out or claim that it adheres to this NSI Code of Practice, unless compliance with the same has been confirmed by NSI and approval granted.

Note: Where any person engages in a licensable activity as designated in the Private Security Industry Act 2001 that person has to be licensed in accordance with that Act. It is an offence to engage in licensable activity without a licence. The Act can be found online at http://www.the-sia.org.uk.

2 Scope

This code of practice gives requirements for companies that provide technical surveillance counter-measures services inside the United Kingdom of Great Britain and Northern Ireland, and Crown Dependencies, including the planning, delivery and reporting of such services.

Note: See also the NSI Regulations and the NSI Guarding scheme approval criteria.

3 Terms and definitions

3.1 **Customer:** individual(s) or a corporate body retaining the services of the organization.

3.2 **Subcontract:** all, or part, of a contract assigned to another service provider, where the subcontracted service provider is responsible for service delivery including the supply and management of their employees in fulfilment of the subcontract.

3.3 **Subcontracted service:** provision of services on behalf of a principal contractor.

3.4 **Subcontracted services provider:** company that is contracted to provide service delivery on behalf of the principal.

3.5 **Technical surveillance counter-measures services:** The service provided to detect the presence of technical surveillance (eavesdropping) devices and hazards and/or to identify technical security weaknesses that could aid in a technical penetration of the customer's premises.

3.6 **Technician:** A person competent to conduct physical and technical searches, using appropriate equipment to detect technical surveillance (eavesdropping) devices.

3.7 **You:** The individual or organization that provides technical surveillance counter-measures services.

4 The organisation

4.1 Structure

You must possess a clearly defined management structure showing effective control and accountability at each level of the operation.

Details of the ownership of the organisation and the principals' curricula vitae must be available. Any unspent criminal convictions or un-discharged bankruptcy of a principal or director must be disclosed on request.

You should operate a complaints management system.

Note: *Guidance is given in BS ISO 10002.*

You must have appropriate registration with the Information Commissioner Office (ICO) in compliance with the General Data Protection Regulation (GDPR) and the Data Protection Act (DPA).

4.2 Finances

You must have sufficient working capital for your requirements. The capital reserves of the organisation must be sufficient for current and planned needs.

You must, under normal circumstances, be able to present two years' audited trading accounts, except if it is starting as a subsidiary of an established organisation, and/or staff experience and substantial financial backing are evident.

You must prepare annual accounts, in accordance with applicable accounting standards. The accounts must include complete details of expenditure and income, and

must be certified by an accountant or solicitor. Accounts must be made available for examination.

4.3 Insurance

You must possess public liability and professional indemnity insurance at a level of cover commensurate with the business undertaken and the number of persons employed.

Attention is drawn to statutory insurance such as employer and vehicle liability insurance.

Where you use sub-contractors, you should ensure there is sufficient insurance cover commensurate with the business undertaken by them.

4.4 Business operating manual

You must operate to a Business Operating Manual covering the topics given in this code of practice. The Business Operating Manual must be so structured that it can be updated easily as circumstances demand.

In the case of an NSI Gold approved company, the Business Operating Manual (Quality Manual) must comply with BS EN ISO 9001.

All your staff should be familiar with the general structure and content of the Business Operating Manual. Each individual should have detailed knowledge of and familiarity with the sections that relate to them and to their work, sufficient to discharge their duties and to carry out their work tasks. We recognise that some sections may not be relevant to all staff. For example, technical work instructions may not need to be issued to office-based staff.

The Business Operating Manual must say how you control administration. It must cover such processes as handling enquiries, preparing quotations, planning and delivering the service, producing reports, and such activities as purchasing and stock control, document and data control, and filing of correspondence and system information. It must contain (or call-up) a code of conduct for staff and suitable health and safety policy statements.

4.5 Document control and records

You must make sure that the Business Operating Manual, work instructions, other documented information appropriate to the Business Operating Manual and all the customer's contractual documents, are authorised and subject to amendment controls.

You must maintain separate records (hardcopy or electronic) for each customer, employee, sub-contractor and supplier.

The records should be held in a secure manner, but should be easily accessible to authorized persons.

Amended or updated records should be identifiable by date and clearly distinguishable from previous versions.

Information stored in an electronic retrieval system should be regularly backed-up and adhere to current GDPR requirements.

You must keep records of contractual documents and of work carried out (including instructions, checklists and results) for a period of two years after a contract has ended.

An employee's basic records (as detailed in BS 7858) ・should be kept for at least 7 years from the cessation of their employment.

Note: *Minimum periods for retention of records can be reviewed if applicable for particular purposes, especially with regard to potential liabilities for civil action.*

You should clearly define the location of records and documentation, both local and centralized. Archived records should be clearly indexed.

4.6 Complaints

You must have a written procedure covering the prompt handling and timely resolution of all complaints, whether from customers, emergency service authorities, or genuine community representatives. You must handle complaints in keeping with your written procedure.

Note: *Further guidance on complaints management can be found in BS ISO 10002.*

4.7 Premises

You must have an administrative office, and/or operational centre, where records, professional and business documents, certificates, correspondence, files and other documents necessary for conducting business transactions must be kept in a secure manner.

5 Resources

5.1 Security screening and personnel identification

As a minimum, you must keep to the recommendations given in BS 7858: British Standard code of practice for security screening of individuals employed in a security environment. You need to have a written procedure covering security screening of personnel, including any sub-contractors. You need to keep records of all screening processes.

Evidence of valid Government Security Clearances, above Counter Terrorist Checks, may be used in lieu of BS 7858 requirements.

You must issue a photo ID card to each member of your staff and to each sub-contractor who represents your company. The photo ID card must clearly give the identity of the holder, the signature of the holder, the name, address and telephone number of the business, and an expiry date.

5.2 Directly employed staff

5.2.1 Selection and screening

All persons undertaking, or having access to, details of technical surveillance counter-measures duties should be selected and screened in accordance with 5.1.

If employees are acquired through a merger or acquisition, you should be satisfied that the recommendations of this sub-clause have been fully met.

They should also be able to demonstrate appropriate skills and competencies sufficient to perform their roles effectively.

Prospective employees should be asked to confirm that there is nothing in their circumstances that would be detrimental to their operational commitments.

5.2.2 Health

You should ensure that the health and physical condition of personnel remains compatible with the duties to which they will be deployed.

Note: *Where there are health and safety risks or medical concerns about personnel, it is reasonable for you to ask that person(s) to undergo a medical examination to ensure fitness for duty.*

5.2.3 Terms and conditions of permanent staff

Employees should be sent a written statement of the terms and conditions of their employment that include details of the following:

a) job title;
b) effective start date;
c) probationary period (if required);
d) provisional period subject to screening (if applicable);
e) pay and allowances;
f) hours and days of work;
g) leave entitlement;
h) conditions of payment during absence through illness;
i) pension entitlement;
j) industrial injury procedures;
k) the address of the organization;
l) equipment supplied;
m) disciplinary and appeals procedures; and

n) terms of notice of termination of employment. Persons should not be required to work hours that could be detrimental to their health, safety or efficiency.

Note: *Attention is drawn to statutory requirements relating to employment, and in particular, to requirements relating to working hours.*

5.2.4 Code of conduct

Note: *This list is not exhaustive and does not necessarily include all actions that could also constitute criminal offences.*

You should issue all personnel with a code of conduct and instruct that the following (including the aiding and abetting of others) constitutes a breach of the code of conduct:

a) neglecting to complete a required task at work promptly and diligently, without sufficient cause;

b) leaving a place of work without permission, or without sufficient cause;

c) making or signing any false statements, of any description;

d) destroying, altering or erasing documents, records or electronic data without permission or through negligence;

e) divulging matters confidential to you or the customer, either past or present, without permission, i.e. breach of confidentiality;

f) soliciting gratuities, or not reporting gifts received, or other consideration from any customer or customer's representative;

g) failure to exercise reasonable care of, or properly account for equipment, property or information received in connection with business;

h) incivility to persons encountered in the course of duties, or misuse of authority in connection with business;

i) conduct in a manner likely to bring discredit to you or the customer, e.g. in relation to cultural diversity and non-compliance with the laws and regulations appertaining to the region of operation;

j) use of equipment or identification without permission;

k) reporting for duty under the influence of alcohol or drugs, or use of these whilst on duty;

l) failure to notify you immediately of any:

1) conviction for a criminal offence including a motoring offence carrying endorsement or fixed penalty;

2) police caution;

3) refusal, suspension or withdrawal (revocation) of a Security Industry Authority (SIA) or other appropriate national licence, if applicable.

m) permitting unauthorized access to a customer's premises;

n) carrying of unauthorized or unlawful equipment, or use of a customer's equipment or facilities without permission; and

o) failure to disclose any circumstances that can involve a conflict of interest (e.g. between themselves and the customer).

5.2.5 Licensing status

Where relevant, you should maintain a record of the current status of any relevant operational licences and conduct regular checks to confirm that employees comply with the terms and conditions of their licence.

5.3 Sub-contractors

Note: *It is recognized that many technicians are sub-contractors.*

5.3.1 General

You should ensure that appropriate written contractual arrangements in place with the sub-contractors.

5.3.2 Initial selection and screening

Although no system of selection can provide absolute security, you should make every endeavour to ensure that the integrity and quality of your sub-contractors is established and maintained.

You should carry out relevant pre-employment enquiries to ensure that only suitably skilled sub-contractors are recruited or added to your database.

You should hold curricula vitae for all sub-contractors on your database.

The initial selection procedure should include a personal interview and should be designed to assess the following:

a) physical ability to carry out the services required;

b) aptitude and demeanour;

c) literacy and verbal communication abilities;

d) personal documentation (proof of name, age, address, etc.); and

e) details of licence and qualifications and other training and additional skills.

You should require the applicant to provide an up-to-date curriculum vitae including:

a) details of career history of not less than five years immediately prior to the date of the application or back to the date of ceasing full-time education; and

b) the names of at least two persons, who may be former employers, from whom a reference can be obtained.

The initial screening should be completed within six weeks and should be considered valid for up to one year from completion of screening.

5.3.3 Subsequent screening

You should carry out subsequent screening at least annually and should include a signed declaration from the sub-contractor detailing any relevant changes in personal and professional circumstances (e.g. training undertaken, qualifications obtained).

5.3.4 Suppliers of sub-contract labour

Where sub-contractors are provided through another organisation, you should ensure that these recommendations have been satisfied by that organisation.

5.3.5 Qualifications of sub-contractors

You should ensure that sub-contractors provided by another organisation:

a) are satisfactorily screened in accordance with BS 7858 or in accordance with 5.3.2;

b) are competent to undertake the work involved;

c) are adequately insured;

d) have individually signed a confidentiality agreement relating to the disclosure of the customer's and your confidential information or material;

e) agree to report immediately to you any alleged or actual contravention of relevant legislation; and

f) are appropriately licensed, where required.

You should retain evidence of items a) to f) above.

5.4 Equipment

5.4.1 Equipment for technical surveillance counter-measures

Note: *This document does not detail specific equipment to be used, this will vary according to the threats and services provided.*

Equipment used must comply with all statutory and regulatory requirements including those for electrical safety, electromagnetic compatibility and the permitted use of wireless frequencies. This includes all necessary markings, which shall be clear, unambiguous and meet all necessary requirements.

You should keep up-to-date with developments in technical surveillance counter-measures and ensure your equipment is fit for purpose.

5.4.2 Test equipment care and maintenance

You must take reasonable and appropriate steps to make sure that essential test equipment is functional and that it gives indications which are accurate within appropriate tolerances. Your procedures for caring and maintaining test equipment need to be in writing as part of the Business Operating Manual.

5.5 Training

5.5.1 General

You should have a clearly defined and documented training policy as part of the Business Operating Manual.

Note: *National Occupational Standards have produced a series of training modules for technical surveillance counter-measures and these should be taken into consideration.*

5.5.2 Induction training

Note: *The contents, timing and duration of induction training are left to your discretion.*

You should provide induction training in matters related to conditions of employment and organizational procedures for all employees. This induction training should be additional to the specific operational training described in 5.5.3. Induction training for directly employed staff should be provided prior to operational duties.

5.5.3 Operational training

You should ensure that all technicians, whether directly employed or sub-contractors, have received the appropriate operational training.

5.5.4 Specialist training

Technicians required to perform specialist duties (e.g. electronic counter-measures, threat assessment) should be trained to the appropriate standard by suitably qualified or competent person(s). Training should be provided on the use of specialized equipment.

5.5.5 Operational familiarization

Where necessary for operational effectiveness, operatives should be given appropriate familiarization training, e.g. update on local culture, law, religion, security forces and political situation.

5.5.6 Team leader proficiency

You should ensure that team leaders are able to demonstrate the skills and experience required in their relevant roles, e.g. in the following areas:

a) leadership skills;

b) operational planning including risk management; and

c) team management.

You should ensure that a team leader understands the importance of:

a) reviewing the performance of individuals and the team;

b) ensuring the implementation of improvements; and

c) recognizing achievements.

5.5.7 Refresher training

You should monitor the effectiveness of all operatives and, if necessary, refresher or remedial training should be provided by suitably qualified or competent person(s) as soon as practicable.

5.5.8 Contingency training

If there is a change in methods, procedures or legislation, you should ensure that operatives are re-trained to a proficient level by suitably qualified or competent person(s). If practicable, training should take place before change is implemented.

5.5.9 Training records

You must keep training records for all staff, and also for any sub-contractors, to demonstrate that appropriate skills have been gained by those undertaking specific tasks. You need to include specific skills needed for office or administration staff.

6 Service provision

6.1 Sale of services

6.1.1 Customer information

Where requested by a potential customer, you should be prepared to provide the following minimum information:

a) your name, address(es) and telephone number(s);

b) details of trade association or professional body membership(s);

c) proof of compliance with industry standards, or details of certification by nationally recognized accreditation bodies e.g. the United Kingdom Accreditation Service (UKAS);

d) legal entity (e.g. limited company, incorporated company, limited liability partnership, sole trader) and your country of registration;

e) your registered number, address and date of registration if you are an incorporated company, or details of partners and an address for legal service of documents if you are a partnership or sole trader;

f) proof of insurance; and

g) data protection notification if appropriate.

6.1.2 Contractual arrangements

You should provide a written quotation. The quotation document should state:

a) the detailed and total costing for the service, and the arrangements for payment;

b) the contract period, along with procedures for termination of the contract;

c) any other contractual requirements made with the customer; and

d) terms and conditions.

The customer should be asked to acknowledge acceptance of the quotation.

Note: *Due to the nature of the sector, where a service provision takes place at short notice a written contract might not always be available.*

As you provide services to detect and/or remove technical surveillance devices, you should not enter into agreements to install such devices.

6.1.3 Contract records

You should retain in the customer file copies of records relating to the contractual agreement between the customer and yourself. These records should be retained and controlled in accordance with section 4.5.

6.2 Due diligence

You should ensure that you know the identity of the customer requesting the service and that the customer has an ethical and legitimate reason for requesting it.

You must adhere to a code of business ethics and selling practice the same as that for other NSI approved companies.

You must not engage in misleading, unfair or pressurised selling techniques and you must adopt and keep to high standards of fairness and integrity.

6.3 Providing the service

6.3.1 Initial customer requirements

You should confirm details of the customer's specific requirements (e.g. what service, who, when, where, how).

6.3.2 Planning considerations

You should consider the following when planning an operation:

a) threat and risk assessment;

b) customer's profile;

c) selection of operatives and allocation of responsibilities;

d) timeframes;

e) locations;

f) resources, communication and logistics;

g) liaison with relevant third parties; and

h) special requirements (e.g. medical).

6.3.3 Customer's approval

You should provide the customer with recommendations and costing for their approval.

6.3.4 Implementation and ongoing assessment

The operation plan should be issued, the team briefed (including in-country awareness training) and the plan implemented.

This should include continued assessment of, and response to, the operational effectiveness of the service.

6.3.5 Completion of task

The operatives should be debriefed and any action points noted and implemented. A record of this should be kept on the customers file.

Where practical, the customer should be debriefed. A record of this should be kept on the customer's file. This should be followed by a written report dependent upon the terms of the contract.

6.4 Threat and risk assessment

You should ensure that the initial threat and risk assessments are conducted by a competent person. These should identify specific operational risks to the customer and the operatives. A record of these assessments should be kept and used for the production of the operational plan.

The threat and risk assessment should be updated dynamically during the operation, as necessary.

6.5 Briefing

All operatives should be briefed in order to ensure that they understand the requirements of the operation.

A briefing should include information on the following:

a) operatives roles and responsibilities;

b) area/ground, e.g. topographical features, places of interest;

c) objective of the operation;

d) levels of threat and risk;

e) local culture, law, religion, security forces and political situation;

f) operational methodology;

g) resources and logistics; and

h) administration and communications.

6.6 Conduct of operation

Note: *It is recognized that a 'team' could comprise a single operative, in which case the responsibilities of team leader and team member would belong to that single operative.*

6.6.1 Your responsibilities

You should:

a) maintain close liaison with the customer as required to ensure any changes that might affect the level of risk are communicated in a timely manner;

b) ensure the resources and control measures allocated to the operation remain appropriate to any change in the level of threat; and

c) provide appropriate communications and support for the team leader during the operation.

6.6.2 Team leader

During the operation the team leader should:

a) maintain a safe environment for the operation;

b) ensure all team members are correctly briefed on any changes to the operation plan;

c) ensure all team members are conducting their duties competently;

d) plan the administration and oversee the welfare of the team (e.g. adequate refreshments and periods of rest); and

e) ensure serviceability of all equipment, vehicles and other modes of transport issued and supplied (see also 5.4.1 and 5.4.2).

6.6.3 Team member

A team member should:

a) conduct their duties competently; and

b) inform the team leader as soon as is practical of any changes which might impact on the effectiveness of the operation.

6.6.4 Operational debriefing procedure

6.6.4.1 General

Debriefs should occur at the end of each operation and, where necessary, at other key times during the operation.

6.6.4.2 Aim of debrief

The debrief should determine the effectiveness of the operation from the perspective of the operational team and, where possible, the customer.

Note: *It is recognized it is not always possible to debrief all team members, or the customer.*

6.6.4.3 Scope of operational debrief

An operational debrief should include a review of all the key briefing factors. It should include a general overview of the operation involving all team members and should identify those areas that worked well and those that needed remedial action. Any comment/feedback from the customer should be taken in to consideration as part of the debrief process.

It is important that notes of any key points should be made, and that any remedial action identified should inform future planning.

6.6.4.4 Customer debrief

Consideration should be given to contacting the customer for their feedback on any commercial and administrative aspects of the operation.

6.7 Reporting

On completion of the operation, you should provide a report of your findings to the customer. This can take the form of a written report or verbal briefing dependent on the terms of the contract.

Example: the report may be formatted to include the following headings:

a) Customer.
b) Location.
c) Date of work.
d) Scope of work.

e) Observations.
f) Recommendations.
g) Conclusions.

Observations and recommendations contained in the report should be based on policies, practices, procedures or requirements against which you compare collected evidence about the subject matter.

Note: *Requirements may include but are not limited to standards, guidelines, specified requirements, and legislative or regulatory requirements.*