CPNI
Centre for the Protection of National Infrastructure

PROCURING THE SERVICES OF A SPECIALIST SECURITY CONSULTANT WHEN UNDERTAKING A PROJECT RELATING TO A BUILT ASSET

Version 7

October 2020

Introduction

Security is an essential element of any project concerning the creation (encompassing planning, design and construction), modification, improvement or disposal of a built asset. Expertise may be required to support in the development and review of: risk assessments; a security strategy; a security plan; and security aspects of the project design, as well as to provide assistance in the procurement, technical design and construction phases. Where the necessary expertise is unavailable in-house, the security or project manager of any significant built asset venture will need to consider procuring the services of one or more specialist security consultants.

CPNI has produced this guide on aspects of sourcing, procuring, tasking and retaining specialist security consultants. It highlights issues that need to be considered when seeking a suitable proposal from such a consultant, ranging from acceptance of the project scope and requirements, to details of resourcing, fees structure and insurance.

CPNI sponsors the Register of Security Engineers and Specialists (RSES) (www.rses.org.uk) which encompasses Generalist Security Advisors (GSA) and Specialist Security Advisors (SSA) in one of eleven different disciplines:

- *Protection against the effects of weapons*
- *Protection against the effects of blast*
- *Electronic security systems*
- *Chemical, biological, radiological and nuclear (CBRN)*
- *Hostile vehicle mitigation*
- *Protection against forced entry*
- *Explosives and weapons search detection*
- *Force protection engineering*
- *Digital built environment*
- *Personnel security (insider threat)*
- *Personnel security (human factor)*

Membership of the RSES is by application, submission of documentation, examination and/or experiential subject peer review. Registered members are given direct access to a wider range of CPNI materials up to OFFICIAL SENSITIVE. Please be aware that if a security consultant is used who does not have access to such materials, the procuring organisation will need to take responsibility for accessing any relevant threat or security information and providing appropriate briefing to the consultant retained. Third-parties wishing to verify the membership categories for an individual or employer, or an RSES member wishing to update membership data, should contact registers@ice.org.uk.

Consultants may also be admitted to the Register of Chartered Security Professionals (charteredsecurityprofessional.org) which has been established by Royal Charter granted to the Worshipful Company of Security Professionals and managed by The Security Institute (security-institute.org/csyp). Chartered Security Professionals make a strategic contribution using their competences in security, practical application, communication, leadership and commitment to ongoing learning and development. Their competence is independently verified through a combination of documentary evidence, qualifications, training, experience and passing a professional peer review.

Another organisation in the field is the Association of Security Consultants (ASC) which has independent security consultants from a range of security backgrounds listed on the UK Register of Independent Security Consultants (www.securityconsultants.org.uk).

The National Cyber Security Centre (NCSC) has its own certification of industry expertise for cyber security, further details of which are available on its website (www.ncsc.gov.uk/articles/about-certified-professional-scheme).

CPNI does not take responsibility for the selection, retention or supervision of security consultants; these are matters for the client, assisted by this guide. Similarly, CPNI has no role in the professional regulation of consultants: any concerns or complaints should be dealt with under the terms of the contract in place with the security consultant and/or be directed to their professional body.

This document comprises a sample of a Request for Proposal that it is recommended a client modifies in line with their specific requirements (further guidance on which is contained within the notes[1] included within the document) and issues to suitable consultants as part of the procurement process.

[1] All notes are provided to assist the Client in completing the document and should be removed prior to the Schedule being issued to the Security Consultant

Security Consultant – Request for Proposal

NOTE[2]:

A Request for Proposal should be provided for each specialist security service required.

Specialist services include:

- *General security advice*
- *Personnel security*
- *Digital built asset & environment security*
- *Protection against the effects of weapons*
- *Protection against the effects of blasts*
- *Explosives and weapon search detection*
- *Electronic security systems*
- *CBRN protection*
- *Protection against hostile incursion*
    - *Hostile vehicle mitigation*
    - *Pedestrian barriers*
- *Force protection engineering*
- *Cyber security*

It is important that a Security Consultant is not asked to, and does not, provide advice outside their area of expertise. As such, establishing the extent of the skills and knowledge of each consultant as part of the procurement process is extremely important in order to ensure that the correct level and range of security services required for the project are obtained. Where a preferred lead consultant lacks expertise in a niche area, they should demonstrate that they have covered that gap by sub-contracting the required services to an appropriately accredited subject matter expert.

*Further information on the skills required for each of these disciplines are available through the RSES (*www.rses.org.uk*) and, in respect of cyber security, the NCSC (www.ncsc.gov.uk/marketplace).*

More general information on the experience and knowledge expected from security professionals is available on The Security Institute website (security-institute.org).

[2] All notes are provided to assist the Client in completing the document and should be removed prior to the Schedule being issued to the Security Consultant

In considering this proposal, all information contained within this document relating to the project shall be treated in the strictest of confidence. Further, the forwarding or discussion of the detail of the document with any external bodies shall not take place without prior approval from the Client.

NOTE:

It is likely that a full confidentiality clause will be required in the contract.

Section 1 – Client Brief

The Client Brief is contained in Appendix A.

Section 2 – The Services to be Provided

The detailed Schedule of Services is contained in Appendix B.

NOTE:

The Schedule of Services should include details of the roles and responsibilities of the Security Consultant to which this document relates.

Section 3 – Programme & Procurement

An initial outline programme is contained at Appendix A.

NOTE:

The Client should also use this section to define their requirements regarding procurement – for example:

"The Security Consultant may be novated to the Main Contractor at the main works contract award, although the Client may wish to retain the Security Consultant.

You should advise whether the novation of your appointment would have any impact on your fees."

Section 4 – Project Structuring

NOTE:

The Client should use this section to set out details as to how the project to which the proposal relates will be structured.

Section 5 – Conditions of Engagement

The Client's form of appointment is contained in Appendix D.

Section 6 – Fees

Fees shall be paid monthly in arrears subject to receipt of a suitable VAT invoice (where applicable) in accordance with a pre-agreed cashflow.

Section 7 – Format of Consultant Response

It is requested that the Consultant's response to this Request for Proposal is structured to address each of the following specific points:

a) Project Overview -

Confirmation that the project scope (Appendix A) is understood and acceptable.

b) Services to be Provided -

Confirmation of acceptance, or otherwise, of the proposed Schedule of Services (Appendix B) and any Contractual Requirements (Appendix C) that may be required.

c) Programme -

Confirmation that the noted timescales are agreed and acceptable.

d) Conditions of Engagement -

Confirmation that the Conditions of Engagement (Appendix D) are agreed and acceptable.

e) Resourcing -

Confirmation of the name and position/grade of each of the persons responsible for the project within the Security Consultant Organisation and the time that they shall dedicate exclusively to the project.

Provision of the name, CV, RSES grade and location of each of the persons it is proposed will work on the project, together with a brief description of their role and time dedicated exclusively to the project.

Statement as to the availability of each member of the team.

Details of all the offices from which services shall be provided.

f) Fee Scheduling -

The fee proposal offered by the Security Consultant for undertaking the services proposed through the project up to and including practical completion and the issue of final certificates (see Appendix E).

Details of the hourly rates at which any additional services will be charged, should lump sum fees not be agreed or should services be required that fall outside the lump sum fee agreement.

The fees shall exclude VAT, where the Security Consultant is VAT registered, but include appropriate allowance for all disbursements and expenses to be incurred by the Consultant and arising from the provision of the services in connection with the project. The allowance shall not include any overseas travel or overnight accommodation associated therewith. Such costs, where previously authorised by the Client in writing, shall be reimbursed at cost upon submission of appropriate VAT receipts.

g) Insurances –

Please provide broker's details of your current policies for:

i. Professional Indemnity
ii. Public Liability
iii. Employer's Liability (where applicable)

NOTE: The Client should specify the minimum amount of professional indemnity and public liability insurance that the Security Consultant should hold.

h) Conflicts of Interest

Please list any potential conflicts of interest that may actually or be perceived to impact your ability to provide the consultancy services fairly and objectively.

i) Other Relevant Information –

For example, any other information you consider relevant in relation to the Schedule of Services (Appendix B).

APPENDIX A

CLIENT BRIEF AND PROGRAMME

NOTE:

This section is to be completed in full by the Client, or their representative, and should contain:

1) *A brief of the nature and extent of work required to be undertaken by the Security Consultant*
2) *A description of the scope of the project*
3) *An initial outline programme for the project*

APPENDIX B

SCHEDULE OF SERVICES

The … [Organisation/Role] shall be responsible for liaising with the Security Consultant and coordinating their activities with those of other members of the Project Team (including any relevant sub-consultants and sub-contractors).

NOTE:

The Client should specify the organisation and role that shall be responsible for liaising with the relevant Security Consultant and coordinating their activities with those of other members of the Project Team.

The Services which the Security Consultant shall provide are as follows:

NOTE:

The Client should delete, amend or add to the requirements set out below as necessary in order to reflect the specific requirements of the project and the specialism of the Security Consultant to which the Request for Proposal relates.

1. ASSESSMENT OF RISKS AND DEVELOPMENT OF RISK MITIGATION OPTIONS

The risk assessment and development of risk mitigation options shall be completed in draft form and sent to the Client for review by …[Date], and finalised for sign-off by the Client by …[Date].

Risk Assessment

The security risk assessment shall take into consideration:

- the project goals and planned programme;
- the technology and processes it is proposed will be used;
- the type of data and information that will be obtained/generated; and
- the lifecycle of the project in relation to all of the identified risk factors.

NOTE 1:

The risk assessment should be undertaken as early in the project as possible in order that appropriate and proportionate mitigation measures can be developed and implemented in a cost-effective manner.

NOTE 2:

A high-level risk assessment should be undertaken as part of the Client's Operational Requirements process[3].

Where the Client is using this Request for Proposal document to procure the services of a Security Consultant to deliver this Operational Requirement, the text under Note 3 below should be used and the text under Note 4 should be removed.

[3] See CPNI website for more information

In addition to the high-level risk assessment contained in the Operational Requirement, risk assessments specific to the different specialist security disciplines should be carried out.

Where the Client is using this Request for Proposal document to procure the services of a specialist Security Consultant in relation to a specific security discipline, the text under Note 3 below should be removed and the text under Note 4 used in its place.

Under these circumstances, the Security Consultant should be provided with a copy of the Client's Operational Requirement documentation prior to the Consultant undertaking their discipline-specific risk assessment.

NOTE 3:

The text below should be used for a Security Consultant procured to deliver a security Operational Requirement, and the text under Note 4 removed.

The assessment shall be summarised in a report which shall include the following:

a) The assets (including data and information) that need to be protected, including those which are deemed critical.

b) Commentary on:

   i. The potential threat actors that may seek to attack or compromise the business' built asset(s), data and information, personnel and/or services provided, and the actions each threat actor may seek to fulfil.

   ii. The vulnerabilities that each identified threat actor may credibly seek to exploit in order to carry out their action.

   iii. The nature of harm, in terms of value and/or loss, that could be caused to the business': assets, including data and information; personnel; and services (whether societal, environmental and/or commercial) as well as to other third parties (for example, citizens), if an identified threat actor was able to successfully exploit a vulnerability.

   iv. The likelihood of a threat actor being able to successfully exploit an identified vulnerability to cause the harm predicted.

c) Review of the area adjacent to the site, and the potential for attacks against neighbouring built assets to impact on the business' built asset, personnel and/or services provided.

d) A summary of the security risks that the business faces.

NOTE 4:

The text below should be used for a specialist Security Consultant in relation to a specific security discipline, and the text under Note 3 removed.

The assessment shall be summarised in a report which shall include the following:

a) Within the specialism to which this document relates, commentary on:

   i. The potential threat actors identified in the security Operational Requirements that, utilising a method of attack within the scope of this specialism, may seek to attack or compromise the business': built asset(s), data and information, personnel and/or services provided.

   ii. The area adjacent to the site, and the potential for attacks against neighbouring built assets to impact on the business' built asset, personnel and/or services provided.

   iii. Previous and existing methods of attack including historical attacks on similar targets, and evolving trends in this area.

   iv. The vulnerabilities that each relevant threat actor may credibly seek to exploit in order to carry out their action.

   v. Credible methods of attack that could be used by a potential threat actor in relation to business': built asset(s), data and information, personnel and/or services provided.

   vi. The nature of harm, in terms of value and/or loss, that could be caused to the business': assets, including data and information; personnel; and services (whether societal, environmental and/or commercial) as well as to other third parties (for example, citizens), if an identified threat actor was able to successfully exploit a vulnerability.

   vii. The likelihood of a threat actor being able to successfully exploit an identified vulnerability to cause the harm predicted.

b) A summary of the risks, within the specialism to which this document relates, that the business faces.

Identification of Risk Mitigation Options

The Security Consultant shall set out the *high-level/specialism-specific* potential risk mitigation options to mitigate the risks identified in the risk assessment, including the nature and scale of resources required for their implementation, and the residual risks that would exist post implementation.

NOTE 1:

The term 'high-level' should be used for a Security Consultant procured to undertake this work as part of a security Operational Requirement, and 'specialism-specific' for a Security Consultant contracted to provide advice within a particular specialism.

The Security Consultant shall detail any linkages required with other specialist security fields, including the potential for compromise of these risk mitigation options measures that may be introduced though exploitation of data and information generated through digital engineering and/or asset management processes.

2. DEVELOPMENT OF A SECURITY PLAN

Risk Assessment Review

If the Security Plan is not being developed immediately after the completion of the specialism-specific risk assessment, the Security Consultant shall undertake an appropriate review of the most recent version of that specialism-specific risk assessment. Where the need for any changes are identified, an updated version of the assessment shall be sent to the Client for approval and sign-off.

The occurrence of this review, including where no changes are identified, shall be recorded within the relevant risk assessment documentation.

This review, as well as any edits to the risk assessment, shall be completed by…[Role].

Risk Mitigation Options Review

Where the specialism-specific risk assessment has been updated, the Security Consultant shall undertake a review of the agreed risk mitigation options, taking an appropriate and proportionate assessment of any changes required, taking into consideration the implications for the cost of the project and the project timetable. Any changes shall be sent to the Client for approval and sign-off.

The occurrence of this review and the decision-making processes, including where no changes are identified, shall be recorded within the relevant risk mitigation documentation.

This review, as well as any edits to the risk mitigation options, shall be completed within… [Timeframe] of the completion of the risk assessment review process.

Any amendments to the risk assessment and risk mitigation options shall be sent to the Client for review by … [Date], and finalised for sign-off by the Client by …[Date].

Development of a Security Plan

Using the relevant risk assessment and risk mitigation options signed off by the Client, the Security Consultant shall prepare a specialism-specific Security Plan. This shall include:

a) A review of any intended security procedures for the built asset(s) and site already identified by the Client.

b) An assessment of the specialism-specific security requirements.

c) The policies and processes required to consistently implement the specialism-specific agreed risk mitigation options and security requirements.

d) Specification for the maximum graphical and non-graphical information for relevant physical assets and systems, or pertaining to security procedures or sensitive operational aspects of the use and management of the built asset(s) that shall be submitted within any planning application and/or provided to any other third party, as well as any specific handling requirements that will be required.

e) Guidance for all other specialists/disciplines involved in the project, sufficient for them to be able to deliver their work to meet the requisite security requirements in a timely and efficient manner.

f) An assessment of the specialism-specific security operational requirements for the completed built asset(s) and/or site.

The Security Consultant shall work with the other security consultants appointed by the Client to produce a draft combined Security Plan.

[Role]…. will be responsible for leading this work and producing a final agreed draft version of the combined Security Plan to submit to the Client.

NOTE 1: The role that will be responsible for leading the development of the Security Plan should be identified.

The combined Security Plan shall also include:

a) An assessment of organisation readiness to implement the proposed security plan.

b) An assessment of the ability of the built asset(s), site and associated systems, policies and processes to counter the scenarios identified in the relevant risk assessments.

c) An assessment of the ability of the business, built asset(s), site and associated systems, policies and processes to function in the event of the type of attack(s) identified in the relevant risk assessments.

The Security Plan shall be completed in draft form and sent to the Client for review by …[Date], and finalised for sign-off by the Client by …[Date].

NOTE 2: The Security Plan should be produced and agreed as early in the project as possible in order that the necessary security measures are built into the project design, including the manner in which information is handled and the requirements placed on the supply chain. It is advised that the Security Plan is completed before the end of the Concept Design phase of the project is reached and prior to the submission of any planning application documentation.

NOTE 3: The Security Plan should be used to assess, evolve and justify the actions to be taken and investments to be made to protect critical assets against security threats.

3. REVIEW OF THE PROJECT DESIGN

Risk Assessment Review

If the Review of the Project Design is not being developed immediately after the completion of the development of the Security Plan, the Security Consultant shall undertake an appropriate review of the most recent version of that specialism-specific risk assessment. Where the need for any changes are identified, an updated version of the assessment shall be sent to the Client for approval and sign-off.

The occurrence of this review, including where no changes are identified, shall be recorded within the relevant risk assessment documentation.

This review, as well as any edits to the risk assessment, shall be completed by…[Date].

Risk Mitigation Options Review

Where the specialism-specific risk assessment has been updated, the Security Consultant shall undertake a review of the agreed risk mitigation options, taking an appropriate and proportionate assessment of any changes required, taking into consideration the implications for the cost of the project and the project timetable. Any changes shall be sent to the Client for approval and sign-off.

The occurrence of this review and the decision-making processes, including where no changes are identified, shall be recorded within the relevant risk mitigation documentation.

This review, as well as any edits to the risk mitigation options, shall be completed within…[Timeframe] of the completion of the risk assessment review process.

Any amendments to the risk assessment and risk mitigation options shall be sent to the Client for review by …[Date], and finalised for sign-off by the Client by …[Date].

Security Plan Review

Where the specialism-specific risk management documentation has been updated and any amendments agreed with the Client, the Security Consultant shall review the specialism-specific Security Plan and combined Security Plan.

This review shall be completed within…[Timeframe] of the completion of the risk management review process.

Where the need for any changes are identified, the proposed amendments shall be sent to …[Role] for collation and for sending to the Client for approval and sign-off.

NOTE 1: The role that will be responsible for leading the development of the Security Plan should be identified.

The Security Consultant shall meet with the Client as required to provide updates and to discuss any issues that impact upon the specialism-specific Security Plan and/or combined Security Plan previously signed off by the Client.

The outcome of all meetings shall be documented, including the decisions made and actions arising, and a copy sent to the Client by the Security Consultant.

Review of the Project Design

The Security Consultant shall:

a) Meet with the relevant Design Team members to review the relevant aspects of the design and assess its compliance with the specialism-specific Security Plan.

b) Meet with other security consultants employed on the project to ensure a consistent, holistic approach to security is taken.

Where any issues are identified, the Security Consultant shall work with other relevant members of the Project Team to find, and agree upon, appropriate and proportionate solutions.

Where necessary, the Security Consultant shall update the specialism-specific Security Plan to reflect the actions agreed with the Project Team.

Where the need for any changes are identified, proposed amendments to the combined Security Plan shall be sent to …[Role] for collation and for sending to the Client for approval and sign-off.

NOTE 1: The role that will be responsible for leading the development of the Security Plan should be identified.

The Security Consultant shall meet with the Client as required to provide updates and to discuss any issues that impact upon the specialism-specific Security Plan and/or combined Security Plan previously signed off by the Client.

The outcome of all meetings shall be documented, including the decisions made and actions arising, and a copy sent to the Client by the Security Consultant.

3. TECHNICAL DESIGN SUPPORT

Risk Assessment Review

If the Review of the Project Design is not being developed immediately after the completion of the development of the Security Plan, the Security Consultant shall undertake an appropriate review of the most recent version of that specialism-specific risk assessment. Where the need for any changes are identified, an updated version of the assessment shall be sent to the Client for approval and sign-off.

The occurrence of this review, including where no changes are identified, shall be recorded within the relevant risk assessment documentation.

This review, as well as any edits to the risk assessment, shall be completed by…[Role].

Risk Mitigation Options Review

Where the specialism-specific risk assessment has been updated, the Security Consultant shall undertake a review of the agreed risk mitigation options, taking an appropriate and proportionate assessment of any changes required, taking into consideration the implications for the cost of the project and the project timetable. Any changes shall be sent to the Client for approval and sign-off.

The occurrence of this review and the decision-making processes, including where no changes are identified, shall be recorded within the relevant risk mitigation documentation.

This review, as well as any edits to the risk mitigation options, shall be completed within…[Timeframe] of the completion of the risk assessment review process.

Any amendments to the risk assessment and risk mitigation options shall be sent to the Client for review by …[Date], and finalised for sign-off by the Client by …[Date].

Security Plan Review

Where the specialism-specific risk management documentation has been updated and any amendments agreed with the Client, the Security Consultant shall review the specialism-specific Security Plan and combined Security Plan.

This review shall be completed within…[Timeframe] of the completion of the risk management review process.

Where the need for any changes are identified, the proposed amendments shall be sent to …[Role] for collation and for sending to the Client for approval and sign-off.

NOTE 1: The role that will be responsible for leading the development of the Security Plan should be identified.

The Security Consultant shall meet with the Client as required to provide updates and to discuss any issues that impact upon the specialism-specific Security Plan and/or combined Security Plan previously signed off by the Client.

The outcome of all meetings shall be documented, including the decisions made and actions arising, and a copy sent to the Client by the Security Consultant.

Provision of Technical Information

During the technical design stage, the Security Consultant shall:

a) Assist in the pre-qualification of potential suppliers and contractors who would be providing services relevant to the security-specialism that the Consultant is contracted to deliver.

b) Prepare the specialism-specific technical information required by the relevant construction teams.

c) Provide support to the design and other specialist teams, as required, within the security-specialism that the Consultant is contracted to deliver.

4. SUPPORT DURING CONSTRUCTION PHASE

Risk Assessment Review

If the Review of the Project Design is not being developed immediately after the completion of the development of the Security Plan, the Security Consultant shall undertake an appropriate review of the most recent version of that specialism-specific risk assessment. Where the need for any changes are identified, an updated version of the assessment shall be sent to the Client for approval and sign-off.

The occurrence of this review, including where no changes are identified, shall be recorded within the relevant risk assessment documentation.

This review, as well as any edits to the risk assessment, shall be completed by…[Role].

Risk Mitigation Options Review

Where the specialism-specific risk assessment has been updated, the Security Consultant shall undertake a review of the agreed risk mitigation options, taking an appropriate and proportionate assessment of any changes that required, taking into consideration the implications for the cost of the project and the project timetable. Any changes shall be sent to the Client for approval and sign-off.

The occurrence of this review and the decision-making processes, including where no changes are identified, shall be recorded within the relevant risk mitigation documentation.

This review, as well as any edits to the risk mitigation options, shall be completed within…[Timeframe] of the completion of the risk assessment review process.

Any amendments to the risk assessment and risk mitigation options shall be sent to the Client for review by …[Date], and finalised for sign-off by the Client by …[Date].

Security Plan Review

Where the specialism-specific risk management documentation has been updated and any amendments agreed with the Client, the Security Consultant shall review the specialism-specific Security Plan and combined Security Plan.

This review shall be completed within…[Timeframe] of the completion of the risk management review process.

Where the need for any changes are identified, the proposed amendments shall be sent to …[Role] for collation and for sending to the Client for approval and sign-off.

NOTE 1: The role that will be responsible for leading the development of the Security Plan should be identified.

The Security Consultant shall meet with the Client as required to provide updates and to discuss any issues that impact upon the specialism-specific Security Plan and/or combined Security Plan previously signed off by the Client.

The outcome of all meetings shall be documented, including the decisions made and actions arising, and a copy sent to the Client by the Security Consultant.

Provision of Information to the Construction Teams

During the procurement and construction stages, the Security Consultant shall:

a) Provide support, within the security-specialism that the Consultant is contracted to deliver, in the process of the procurement of contractors, including:

    i. Finalising specialism-specific technical information.

    ii. Clarification of any technical issues.

    iii. Review of relevant aspects of submitted tenders.

    iv. Assisting in relevant aspects of the selection process.

b) Finalise the specialism-specific technical information required by the relevant construction teams.

c) Advise upon, and review, the security aspects of the technical specifications produced by others, within the specialism that the Security Consultant is contracted to deliver.

d) Monitor, and ensure the satisfactory completion of the implementation of the relevant agreed risk mitigation measures and delivery of those measures against the requirements of the Security Plan.

e) Provide support to the design, construction and other specialist teams, as required, within the security-specialism that the Consultant is contracted to deliver.

The Security Consultant shall meet with the Client as required to provide updates and to discuss any issues arising.

The outcome of all meetings shall be documented, including the decisions made and actions arising, and a copy sent to the Client by the Security Consultant.

A record of recommendations, issues, occurrence of monitoring activity, including the decisions made and actions arising, and the satisfactory completion of measures, where applicable, shall be made and a copy sent to the Client by the Security Consultant.

APPENDIX C

OTHER CONTRACTUAL REQUIREMENTS

To be added by client

APPENDIX D

DEED OF APPOINTMENT AND FORM OF APPOINTMENT

To be added by client

It is recommended that a proportionate approach is taken to the contracts set up for security consultants, with a balanced approach to risk and liability which reflects that many security consultants are within small and medium-sized enterprises.

APPENDIX E

THE FEE

Project Fee

The lump sum shall be split in accordance with the stages described on the cashflow and includes the attendance at meetings during each phase.

Expenses

Fees are quoted inclusive of all normal expenses. Additional costs associated with travel and subsistence outside the UK, at the Client's request and subject to the Client's prior written approval, shall be recharged at cost.

Fee Summary

Project Fee **£**

The lump sum fee for completing the services (exclusive of VAT) **£**

Hourly Rates

Provide Hourly Rates (to include all expenses) for all grades of personnel: -

Principal	**£**
Associate / Project Director	**£**
Other (please list below)	**£**