CPNI
Centre for the Protection of National Infrastructure

ice
Institution of Civil Engineers

RSES Guidance

Institution of Civil Engineers

Register of Security Engineers and Specialists (RSES)

Contents

Please note that the document has been revised at several occasions:

Revision 7 – *Criteria have been modified. No changes relate to procedures. Principal changes are: The removal of Expeditionary Force & Project Management from the specific criteria of General Security Member****. Revision 8 -*** *Criteria have been modified. No changes relate to procedures. Principal changes are: Minor criteria updates to Category A, Protection Against the Effects of Weapons and Category B, Protection Against the Effects of Blasts.* ***Revision 9*** *– Criteria have been modified. No changes related to procedures. Principle changes are: The addition of Category H, Force Protection Engineering.*
Revision 10 - *No changes related to procedures. Principle changes are: addition of Digital Built Environment and Personnel categories.*
Revision 11 - *Principle changes are Grades A, B and C are now referred to Technician Member, Member and Principal Member grades. Minor criteria updates to GSA and ESS. . Category E, Pedestrian Barriers, and Category F, Hostile Vehicle Mitigation merged into one Category E, HVM and Perimeter Pedestrian Barriers. Clarification on admittance at lower grade than applied for. Clarification on Project Report requirements. Updated Engineering Council Professional Competences for EngTech, IEng and CEng.*
Revision 12 *– Principal changes are: Revision to the title and criteria of Category E: HVM and Pedestrian Barriers to become HVM only. Introduction of Category F: Protection Against Forced Entry, Revisions to the categorys' introductions. Revised guidance for candidates applying for non-engineering categories (Category K and K). Guidance for the application and approval of primary and secondary categories as listed on the RSES Company Competence List. Guidance related to security mindedness and clearance of content for an RSES application.*

1 Introduction

1.1
Security engineering encompasses the broad range of specialist engineering and applied sciences that directly contribute to security. Security engineering is generally defined as 'the design and application of physical, personnel and cyber protective security measures to protect assets and operations against malicious attacks such as terrorism, espionage and crime'.

1.2
The Private Security Industry Act 2001 was enacted in 2002 and established the Security Industry Authority (SIA) for mandatory licensing of the UK security industry. The underlying aim of the Register of Security Engineers and Specialists (RSES) is to protect the public by ensuring that those providing security functions are correctly trained, certified competent, checked for criminal activity and subject to relevant continued professional development. However, the demand for a discernible benchmark of professional quality is being addressed through professional registers.

1.3
The RSES has been established to promote excellence in security engineering and those fields which directly contribute to security. It provides a benchmark of professional quality against which its registrants have been assessed. Registration is open to engineers, applied scientists and specialists who apply their knowledge to securing the built environment and infrastructure.

1.4
The RSES is sponsored by the Centre for the Protection of the National Infrastructure (CPNI) and administered by the Institution of Civil Engineers (ICE). It offers potential clients and insurers the assurance that registrants have achieved a recognised competence standard through a professional review process. Registrants are required to accept a code of ethics and have a commitment to Continuing Professional Development (CPD).

1.5
Within the register's categories, candidates may apply at one of three levels which are broadly equivalent to technician, incorporated and chartered status, hereafter referred to as Technician Member, Member and Principal Member grades respectively.

1.6
Registrants are encouraged to use the descriptor 'Technician Member / Member / Principal Member of the RSES' in their professional correspondence. Those companies employing registrants are invited to include the categories at Member and Principal Member grade, under which there employees are listed, on the RSES Company Competence list

1.7
Registrants are not listed in open-source documentation, but if clients want to verify whether an individual is a Technician Member / Member / Principal Member of the RSES they can contact registers@ice.org.uk.

1.8
Registrants will have a sound knowledge and understanding of scientific/engineering/technical principles. They will also have experience of providing advice on security infrastructure in the general security environment or one of the specialist fields.

1.9
To be accepted on the register you must:

- Be professionally qualified with an Engineering Council licensed professional institution, e.g. Institution of Civil Engineers (ICE), at EngTech, IEng or CEng level, or with other relevant institutions, e.g. BCS, The Chartered Institute for IT. Please contact registers@ice.org.uk for further details.

or

- If you are not professionally qualified, you will be expected to demonstrate the generic competences for the relevant grade, A, B or C, as shown in Annex B. You must also hold the relevant academic base as shown in Annex F.

or

- If you are not professionally qualified and do not possess the relevant academic base for the grade you wish to obtain you may apply via the RSES Technical Report Route. Please refer to RGN15, RSES TRR for further details.

- Be successful at the RSES assessment

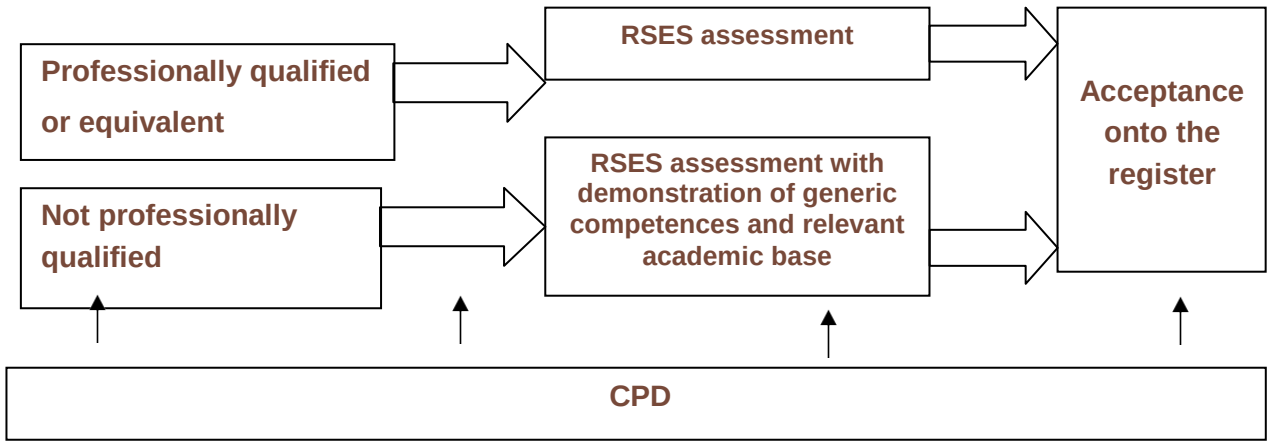

Figure 1- Registration process

Success at the RSES assessment allows you to describe yourself as one of the following:

J Smith *Professional Qualifications*
Technician / Member / Principal Member of the RSES

1.10
Registrants shall be bound by the rules of professional conduct of their host Institution. Registrants will also be bound by the Code of Ethics in Annex A. Registrants who breach the relevant code may be removed from the register.

2 Register categories

2.1
Candidates may apply as either a General Security Adviser (GSA) or as a Specialist Security Adviser (SSA).

Those wishing to apply as a GSA will need to demonstrate a broad experience of security engineering. Those wishing to apply as an SSA will need to demonstrate specialist expertise in one of the following categories:

A Protection against the effects of weapons
B Protection against the effects of blast
C Electronic security systems
D CBRN
E Hostile vehicle mitigation
F Protection against forced entry
G Explosives and weapons search detection
H Force protection engineering
I Digital built environment
J Personnel security (insider threat)
K Personnel security (human factor)

When completing the Expression of Interest form, or the application form for a full application candidates should also indicate only one grade they wish to be assessed (Technician, Member or Principal). It should be noted that GSA candidates will only be admitted to the register at Member or Principal grades. Those candidates advised to submit an application via the RSES TRR will be invited to apply as a GSA only.

2.2
The generic engineering competences for registrants for all grades are set out in Annex B. Candidates who are professionally qualified will have already demonstrated these, or similar, attributes.

2.3
For the personnel categories J, Insider Threat, and K, Human Factor candidates need only demonstrate the application of their specialist knowledge and expertise in Personnel Security in the built environment, as set out in Annex C. They are not required to demonstrate engineering technical knowledge or expertise at assessment or through validation of accredited UK Spec academic qualifications.

2.4
The specific competences for registrants for all grades are set out in Annex C. A glossary of acronyms is attached at Annex D.

2.5
As part of this process a sponsor, who is a registrant at Technician, Member or Principal Member grade of the register, is required to assist the candidate. Further details on the application process are set out in Annex E. Sponsors must be the same grade or a higher grade than the candidate's grade applied for.

2.6
If a candidate does not have a suitable sponsor, they should contact registers@ice.org.uk for assistance.

2.7
A summary of the eligibility criteria and requirements is set out in Annex F.

3 The assessment

3.1
Assessments are held to assess candidates for inclusion on the register.

3.2
The assessment consists of two parts:

- The submission of an application and associated documents
- An interview with two assessors appointed by ICE For further details of the assessment, see Annex E

4 Continuing Professional Development (CPD)

4.1
Continuing Professional Development (CPD) is defined as the systematic maintenance, improvement and broadening of knowledge and skills, and the development of personal qualities necessary for the execution of professional and technical duties throughout your working life.

4.2
As part of your assessment you will be assessed on your commitment to CPD both to date and in the future. RSES recommends the use of the "CPD Cycle" promoted by many professional institutions, details of which can be found in ICE's Continuing Professional Development Guidance). The planning and recording of CPD can best be demonstrated by regular use of a Development Action Plan (DAP) and a Personal Development Record (PDR), templates of which are available in the CPD guidance. Alternatively, similar documents containing the same information, which are available from other institutions, can be used.

4.3
You should plan to achieve a well-balanced programme of CPD, including technical, managerial and professional topics but with an additional emphasis on the category of the register to which you are applying. When applying for the RSES, you should ensure that you have kept your skills and experience up-to-date particularly in your specialist area, in order to maintain your knowledge.

4.4
Candidates will be required to demonstrate CPD based on the grade of registration they are pursuing:

- Technician Member: CPD plans and records for the last two years
- Member: CPD plans and records for the last three years
- Principal Member: CPD plans and records for the last four years

5 Post registration CPD

5.1
After registration you will be required to plan and record your CPD. This should be in accordance with the requirements of the registrant's host institution and demonstrate a well- balanced programme, including technical, managerial and professional topics, with a specific emphasis on security and its related specialisms.

5.2
Should you not be professionally qualified, you can find out how much CPD you should undertake and what constitutes suitable CPD by referring to ICE's Continuing Professional Development Guidance.

5.3
Biennially, the registrar may ask you to provide details of both your CPD plan and record. Both will be subject to review. Submitting incomplete or inadequate CPD details could result in your removal from the register.

6 Post registration professional institution membership

6.1
Registrants are expected to retain membership of their host professional institution as noted in section 1.10 above. Failure to do so may result in removal from the register.

7 Register listing and the verification of additional categories

7.1
CPNI publishes an RSES Company Competence List which shows the categories of registration in which the companies' employees have been formally assessed ('peer-reviewed') as competent to work. In addition to the peer- reviewed, or primary, category the list also identifies secondary and additional primary categories, at either Member or Principal Member grade only, where the registrants are considered competent to work.

7.2
The system of listing additional categories recognises that security is multi-disciplinary in nature and consequently registrants at all grades may have experience in more than one discipline. It is also part of the register's commitment to continuing professional development.

7.3
For clients wishing to use the table, the data is provided by the registrants currently employed within each company at the time of publication. It is recommended that those wishing to engage companies to supply security consultancy services ask for confirmation of their employees' categories beforehand as the registrant's current employment may have changed.

7.4
Third-parties wishing to verify the registration categories for an individual or employer, or a registrant wishing to update registration data, should contact registers@ice.org.uk.

Application for additional primary and secondary categories

7.5
Registrants at Member or Principal Member grade of the RSES are invited to submit further evidence of their competence in an additional four primary or secondary categories for assessment.

There will be a six month grace period (1 May to 1 November 2018) for existing registrants to submit one Category Review form per category to retain any secondary categories on the company competence list. After this time, any secondary categories not applied for will be removed from the list.

Secondary and additional primary categories can be applied for at or below the registrant's grade of registration.

Registrant's CPD records should demonstrate continuing professional development in all the categories held.

Retaining or applying for a secondary category

Submission of a Category Review form (including a 500 word supporting statement).

Applying for additional primary categories

- Submission of a Category Review form, including a 1000 word supporting statement
- An experience report relevant to the category applied for (2000 words for Principal Member grade and 1000 words for Member grade)

Primary category experience report

The experience report should describe the structured training and experience the registrant has gained, including the tasks undertaken. It must not be a mere inventory, although it should set out the development of the registrant's career and the precise positions they have occupied. It is essential the registrant's personal experience is emphasised together with their degree of responsibility.

For both secondary and primary categories, the documentation is assessed by a pair of trained assessors.

It will cost £30 to retain or apply for a secondary category, or apply for an additional primary category.

Annex A

Code of Ethics

All registrants of the Register of Security Engineers and Specialists:

i. Will have regard for the health, safety and welfare of the public, and for the environment, in their professional practice.

ii. Will only undertake work which they are competent to do.

iii. Will demonstrate integrity, honesty, fairness and objectivity in all their professional dealings.

iv. Will adhere to all statutes, regulations and by-laws pertaining to their area of practice.

v. Will safeguard and enhance the honour, dignity and reputation of the Register of Security Engineers and Specialists.

vi. Will be expected to undertake and maintain CPD, with emphasis on those RSES categories publicly listed, and develop their professional knowledge, skills and competence on a continuing basis and give all reasonable assistance to further the education, training and continuing professional development of others.

Annex B

Attributes of a registrant - generic competences

B1.1 The following are the core attributes that form the foundation for the specialist competences. Candidates who are professionally qualified at technician, incorporated or chartered (or equivalent) levels with professional bodies or institutions will be deemed to have satisfied these competences.

Technician Member grade (technician)

Attribute Group	Engineering/Scientific/Technical technician
A. Use engineering knowledge and understanding to apply technical and practical skills. **Use engineering knowledge and understanding to apply technical and practical skills.**	This includes the ability to: **A1** Review and select appropriate techniques, procedures and methods to undertake tasks. **A2** Use appropriate scientific, technical or engineering principles
B. Contribute to the design, development, manufacture, construction, commissioning, operation or maintenance of products, equipment, processes, systems or services.	In this context, this includes the ability to: **B1** Identify problems and apply appropriate methods to identify causes and achieve satisfactory solutions. **B2** Identify, organise and use resources effectively to complete tasks, with consideration for cost, quality, safety, security and environmental impact
C. Accept and exercise personal responsibility.	This includes the ability to: **C1** Work reliably and effectively without close supervision to the appropriate codes of practice **C2** Accept responsibility for work of self or others **C3** Accept, allocate and supervise technical and other tasks
D. Use effective communication and interpersonal skills	**D1** Use oral, written and electronic methods for the communication in English* of technical and other Information **D2** Work effectively with colleagues, clients, suppliers or the public, and be aware of the needs and concerns of others, especially where related to diversity and equality.

E. Make a personal commitment to an appropriate code of professional conduct, recognising obligations to society, the profession and the environment.	**E1** Comply with the Code of Conduct of your institution. **E2** Manage and apply safe systems of work. **E3** Undertake engineering work in a way that contributes to sustainable development. This could include an ability to operate and act responsibly, taking account of the need to progress environmental, social and economic outcomes simultaneously **E4** Carry out and record CPD necessary to maintain and enhance competence in own area of practice including: ▪ Undertake reviews of own development needs ▪ Plan how to meet personal and organisational objectives ▪ Carry out planned (and unplanned) CPD activities ▪ Record and maintain evidence of competence development ▪ Evaluate CPD outcomes against any plans made ▪ Assist others with their CPD **E5** Exercise responsibilities in an ethical manner.

*Any interviews will be conducted in English, subject only to the Welsh Language Act 1993 and any regulations which may be made in implementation of European Union Directives on free movement of labour.

Member (incorporated) and Principal Member grades (chartered)

Attribute Group	Principal competences (chartered) – two columns combined	
	Member Grade Attributes (incorporated)	**Principal Member Additional competences to be added to previous column for Member**
1. Knowledge and understanding of engineering	**A** Maintain and extend a sound theoretical approach to the **application** of technology in engineering practice. **B** U**se** a sound evidence- based approach to problem solving and be able to contribute to continuous improvement.	**C** Maintain and extend a sound theoretical approach in **enabling the introduction and exploitation** of new and advancing technology. **D Engage** in the **creative** and **innovative** development of engineering technology and continuous improvement systems.
2. Technical and practical application of engineering	**A Identify,** review and select techniques, procedures and methods to undertake engineering **tasks**. **B Contribute** to the design and development of engineering solutions. **C** I**mplement** design solutions and **contribute** to their evaluation.	**D Conduct** appropriate research, relative to design or construction and appreciate its relevance within own area of responsibility. **E** Undertake the design and development of engineering solutions and **evaluate** their effectiveness. **F** Implement or construct design solutions and evaluate their effectiveness.
3. Management and leadership	**A Plan** for effective project implementation. **B Manage** the planning and organization of tasks, people and resources. **C Manage** teams and develop staff to meet changing technical and managerial needs. **D Manage** quality **processes**.	**D** Plan **direct and control** tasks, people and resources. **E Lead** teams and develop staff to meet changing technical and managerial needs. **F Continuous improvement** through quality management.
4. Independent judgement and responsibility	**A** Identify the limits of **personal** knowledge and skills. **B** Exercise sound **independent engineering judgement** and take responsibility.	**C** Identify the limits of a **team's** skill and knowledge. **D** Exercise sound **holistic independent judgement** and take responsibility.

5. Commercial ability	**A** P**repare** and control budgets. **B** Use **sound knowledge** of statutory and commercial frameworks within own area of responsibility and have an appreciation of other commercial arrangements.	**C** Demonstrate **sound judgement** on statutory, contractual and commercial issues in relation to your area of responsibility.
6. Health safety and welfare	**A** A **sound knowledge** of legislation, hazards and safe systems of work. **B** M**anage** risks. **C** M**anage** health, safety and welfare within own area of responsibility.	**D** L**eading** continuous improvement in health, safety and welfare.
7. Sustainable development	**A** A sound knowledge of sustainable development best practice. **B Manage** engineering activities that contribute to sustainable development	**C Leading** continuous improvement in sustainable development.
8. Interpersonal skills and communication	**A Communicate** well others at all levels including effective use of English orally and in writing. **B Discuss** ideas and plans competently and with confidence. **C** Effective personal and social skills. **D Manage** diversity issues	**E C**ommunicate new concepts and ideas to **technical and non-technical colleagues** including effective use of English (1) orally and in writing.
9. Professional commitment	**A** Understanding and compliance with the RSES Code of Conduct. **B** Plan, carry out and record CPD and encourage others. **C** Engage with RSES activities. **D** Demonstration of appropriate professional standards, recognising obligations to society, the profession and the environment. **E** Exercise responsibilities in an ethical manner.	

(1) All RSES assessments will be conducted in English, subject only to the Welsh Language Act 1993 and any regulations which may be made in implementation of European Union Directives on free movement of labour.

Annex C: Specific Criteria

Attributes of a Registrant - Specific Competences

C1.1 The following are the specific competences for each category and grade of registration.

GENERAL SECURITY ADVISOR	
Introduction	This category exists at Member and Principal Member grades only. General Security Advisers are likely to have strengths in particular areas, e.g. risk assessment, security surveys and audits. They should be knowledgeable in the process and application of measures for the Protection of Assets in the widest sense and are likely to have experience of most of the specialist competence areas. They should be able to provide technical information to specialists and also be able to communicate clearly with non-specialists. The scope and criteria for these areas are set out below. Interviewers will exercise their judgements on the range and balance of competences of each candidate. Candidates for GSA should particularly: • Have an academic knowledge base (preferably a formal qualification in a relevant subject) • Have broad experience of most of the specialist areas • Be able to analyse threat information from both open sources and the intelligence community • Be able to specify general threat mitigation requirements and assess the cost/benefits from possible mitigation measures • Be able to provide technical threat information so that specialists can develop detailed mitigation measures • Be able to provide reports that are comprehensible to non-specialists If you do not have the appropriate educational base through formal academic qualifications, the RSES Technical Report Route (TRR) may allow you to use the equivalent academic knowledge gained by other means, including through your work experience, without completing a period of formal study. Please contact registers@ice.org.uk for further details.
Scope	General Operational Requirements (OR level 1) – User Requirement Document Ability to conduct, interpret, apply and develop threat and risk assessments Risk Assessment Stage I: Business impact analysis

	Risk mapping/nodal mapping Critical dependencies/catastrophic failure modes Identify single points of failure Knowledge & risk mitigation methods Understanding value (cost to business) Threat vulnerability assessment = Risk scoring Stage 2: Mitigation methods Concept Design Operational requirements Assessment of residual risk Project Management Ability to quantify and explain weapons effects including cyber effects that apply to the identification of single points of failure including blast, fragmentation, heat/incendiary and earth shock <u>Types of asset</u> Built environment Existing and new buildings/installations/centres in the public and private sectors Infrastructure – e.g. communications, utilities, ports, airports, road and rail networks Stadia, shopping malls, hospitals, government buildings, financial centres, residential centres, iconic sites Planes/vehicles/ships/trains Workforce, contractors, visitors and people within the risk environment	
	Surveyor: <u>Security surveyor role</u> Set OR assumptions and limits Obtain threat assessment from others/Conduct Threat Assessments Liaise with risk assessors/Conduct Risk Analyses. Desktop survey Physical survey (visual/structural) Electronic and physical security measures/ Protection of Assets Soft security measures – i.e. personnel and procedures. Recommendations/countermeasures. Counter-espionage Note: This is part of Threat Assessment and Risk Analysis.	Surveyor: <u>Incident Investigation</u> Gather information from others Liaise with risk assessors Liaise with forensics (where applicable) Collate/gather information & evidence Apply knowledge of cyber and weapons effects and survey evidence to the collated evidence Liaise with emergency services & other security specialists Analyse & evaluate findings Report & recommendations

	Member	Principal Member
Knowledge criteria	The following in reasonable breadth and depth: Threat assessment methods Risk assessment methods Knowledge of weapons effects Business processes/practices (understanding value) Security processes/practices Impact analysis (critical dependency) Tools (risk scoring) and their limitations Mitigation measures (cost/benefit analysis) Relevant contracts, standards & guidelines Understand technical aspects of security measures/proposals	The following in substantial breadth & depth: Threat assessment methods Risk assessment methods Knowledge of weapons effects Business processes/practices (understanding value) Security processes/practices Impact analysis (critical dependency) Tools (risk scoring) Mitigation measures (cost/benefit analysis) Relevant contracts, standards & guidelines Can engage security professionals in technical discussion
Competence criteria	Application of threat and risk assessment theory (see above) to a targeted range of real situations Can apply existing approaches and responses to situations Good communication skills Can produce standard reports including OR documentation with the addition of analysis based on a range of skills defined in the scope Can produce security operational procedures from templates with the addition of analysis based on the range of skills defined in the scope Can carry out routine surveys and audits	Application of threat and risk assessment theory (see above) to a wide range of real situations Can develop new approaches and responses to new situations Project management Can engage other security specialists in technical discussion Can advise senior non-technical personnel on complex technical issues Can produce high quality reports including OR documentation with the addition of analysis based on a wide range of skills defined in the scope Can produce detailed security operational procedures from a clean start with the addition of analysis based on a wide range of skills defined in the scope Can carry out complex surveys and audits

CATEGORY A: PROTECTION AGAINST THE EFFECTS OF WEAPONS

Introduction	Candidates for RSES Accreditation in the field of Protection Against the Effects of Weapons will need to be able to demonstrate strengths in (at least) the following areas; a knowledge of small arms, military weapons systems, improvised weapons (including improvised explosive devices of various sorts, e.g. rockets and mortars), knives and blunt instruments. This category specifically requires candidates to be able to show a practical understanding of the use of weapons including the properties of different variants and the ability (at Member and Principal Member grades) to calculate range, velocity, trajectory, etc. It also includes an understanding of the factors involved in assessing different possible firing points/baseplate locations, etc. Candidates are expected to show applied knowledge (qualitative and quantitative) of the effects of these weapons (impact damage, penetration, perforation, detonation, air shock, ground shock, hydraulic shock, heat, ricochets etc.) They are also expected to understand how target materials can be introduced or upgraded to mitigate these effects on building materials, infrastructure, solid/rocks, water, vehicles, aircraft, ships, trains etc. They will also appreciate when weapons effects can be credibly calculated and when testing is necessary. They will have knowledge of appropriate test standards. This category is available at all three grades. At Technician Member grade, candidates will have knowledge and experience of carrying out tasks such as blast and/or ballistic testing. Candidates at Member grade should, in a holistic security context, be able to apply knowledge of weapons characteristics, test data, etc. to devise suitable mitigation measures, and specify recognised testing as necessary. At Principal Member grade, this knowledge and experience will be more extensive and will enable the candidate to characterise new weapons, develop new materials or mitigation measures and devise suitable new test procedures and standards.

Scope	<u>General</u> Operational Requirements (OR levels 1 and 2) – User Requirement Document Ability to interpret, apply and develop threat and risk assessments <u>Weapons</u> Small arms, military weapons systems, improvised weapons (IEDs, incendiary devices and mortars), non-conventional weapons, knives and blunt instruments <u>Factors</u> Properties of weapons, properties of ammunition, range/trajectory/velocity, location of potential firing points <u>Weapons effects</u> Projectile characteristics (bullets and fragments), projectile penetration, detonation, impact/damage, air shock, ground shock, water shock, ricochets and heat/incendiary effects <u>Targets</u> Windows/glass, building materials (concrete/masonry/metals/other), infrastructure/utilities, geotechnical materials, soils, water (as defence), water (as means of transport), personnel, vehicles/planes/ships/trains <u>Protection</u> Armouring materials (metal/ceramic/glass/composite) Vehicle armouring Body armour Protection/defence, cover from fire/cover from view <u>Design</u> Construction technology, codes & standards, design assumptions, associated risks, design innovation <u>Tests, trials, reports</u> An ability to research, interpret and apply results from tests, trials and reports

	Technician Member	Member	Principal Member
Knowledge Criteria	Basic – small arms, bomb fragments Basic – windows/glass, building materials Awareness of other weapons & targets Basic knowledge of construction technology and its interaction with weapons effects Design detailing	In depth – small arms, bomb fragments In depth – windows/glass, building materials Awareness of other weapons & targets Construction technology & design principles and its interaction with weapons effects	Knowledge of weapons effects Balance between in-depth knowledge of own specialities and awareness of all other types Awareness of practical use of weapons Construction technology & design principles and its interaction with weapons effects
Competence Criteria	Can identify basic weapons effect problems, and devise solutions Carry out tests and trials Write and present basic reports Prepare component designs Prepare drawings and specifications	Can identify standard weapons effect problems, and devise solutions Manage tests and trials Write and present complex reports Prepare system designs Prepare drawings and specifications	Can identify complex weapons effect problems, and devise solutions Can develop new approaches and responses to new situations Can engage security professionals in technical discussion Can produce high quality reports

CATEGORY B: PROTECTION AGAINST THE EFFECTS OF BLASTS

Introduction

Security engineers specialising in blast effects and analysis are likely to have strengths in particular areas, e.g. the derivation of blast loading and the effects of the blast on various materials/elements. They should be knowledgeable about the process and application of blast protection measures for the protection of assets. They should be able to provide technical information to specialists and also be able to communicate clearly with non-specialists. The scope and criteria for these areas are set out below. Assessors will exercise their judgements on the range and balance of competences of each candidate.

Candidates specialising in blast effects should particularly:

- Have a detailed knowledge of blast loading
- Have experience of the response of elements including:
  - Concrete
  - Steel
  - Glass
  - Masonry
- Be able to undertake dynamic analysis

Candidates should also be able to:

- Specify blast mitigation measures and assess the cost/benefits from possible mitigation measures
- Provide specification information, so that contractors/subcontractors can install detailed mitigation measures
- Provide reports that are comprehensible to non-specialists

This category is available at all three grades

Scope	General Operational Requirements (OR levels 1 and 2) – User Requirement Document Ability to interpret, apply and develop threat and risk assessments General awareness of weapons effects including blast, fragmentation, heat/incendiary and earth shock Explosives Military, commercial, improvised, fuel/air, incendiary, nuclear Explosive effects Air blast, gas effects, fireball, thermal, radiation, ground shock, cratering, fragments (primary, secondary), water shock, brisance, human effects Propagation Transmission by pressure waves (including reflection & refraction), including impulse effects, clearing, and internal explosions with/without venting In different media: air, water, ground (soil or rock), and other solids liquids and gases Material properties Loading rates, high strain rates, brittle/ductile, destruction failure point Material types Masonry, glass, concrete, metals, timber, plastics, composites, soils, water, rocks Tests, trials, reports An ability to research, interpret and apply results from tests, trials and reports Analysis Methodologies Use of accepted charts, manuals (and their simple blast evaluation programs) and test data Use of hydrocodes for blast parameter evaluation Use of single degree of freedom analysis, and other simple approximations Use of finite element analysis (linear and nonlinear) and Eulerian/Lagrangian coupled models Design Construction technology, design assumptions, consequence of failure, outline design, detailed design, codes & standards, dynamic response of structures

	Technician Member	Member	Principal Member
Knowledge Criteria	Awareness of blast waves and their consequences Awareness of specialist issues & terminology Basic knowledge of construction technology Design detailing Basic knowledge of explosives types	In-depth knowledge of military, commercial & improvised explosives, air blast Awareness of other factors Construction technology and design principles, codes & standards with respect to blast effects	In depth knowledge of military, commercial & improvised explosives, explosives effects, materials, dynamic response, design Awareness of other factors
Competence Criteria	Contribute to and support tests and trials Write and present basic reports Prepare component designs Prepare drawings and specifications	Manage tests and trials Write and present complex reports Prepare system designs Prepare drawings and specifications	Can identify blast problems, and devise solutions Can develop new approaches and responses to new situations Can engage security professionals in technical discussion Can produce high quality reports

CATEGORY C: ELECTRONIC SECURITY SYSTEMS

Introduction	This category covers candidates who are practising in the design, selection, implementation and maintenance of electronic security systems. Typically, such systems would include (but are not limited to); Closed Circuit Television, electronic access control, perimeter and intruder detection systems. Furthermore, this category includes software and hardware platforms that integrate electronic security systems, i.e. video management and physical security integration systems. This category is available at all three grades.
	Items highlighted in *italics* are detailed as examples to support the scope detail. <u>General Requirements</u> Ability to interpret, apply and develop electronic security systems mitigation measures using threat and risk assessments and/or Strategic Security Masterplans. Ability to develop a client's brief and work within a defined scope of deliverables. Apply a security mindedness approach i.e. PAS 1192-5 to the use and information sharing of digital design tools, manufacture, installation and operate cycles. Information security principles and cyber considerations <u>Operational Requirements</u> <u>Level 1</u> Ability to define Level 1 operational requirements (OR's) and how these are to be addressed. Use of modelling tools such as : ▪ *Threat assessments, schedule of assets, locations, history of attacks, criteria for success.* ▪ *Strategic consideration of electronic and other counter measures* ▪ *Impact of systems failures* Consider the impact of: ▪ *Human factors i.e. insider threat i.e. HOmER)* ▪ *Information security and general cyber awareness and threats*

Scope	Level 2 (Concept Outline) Ability to interpret Level 1ORs and how these are addressed with utilisation of electronic security measures and produce a Level 2 OR for the following systems: ▪ Feasibility of deploying systems to address L1 requirements : CCTV, IAHS, PIDS, AACS, lighting systems or other appropriate security technology based systems ▪ Security management (SMS), Video Management (VMS) & Physical Security Management (PSIM) systems ▪ Control rooms, ergonomics and human factors ▪ Detailed consideration of asset location and, criteria for success ▪ Consideration of specific electronic and other counter measures ▪ Impact of individual and combined systems failures; both in a sequential and random collective nature ▪ Security 'mindedness' in terms of the design-construct cycle and how design & performance information is appropriately handled and secured during its lifetime ▪ Human factors in terms of threats to system operation Consider several possible alternative solutions and systems that fulfil required OR's / project deliverability, together with their performance metrics. Schematic Design Stage (Concept Definition) Ability to interpret Level 2 Operational Requirements (OR's). Consideration of factors affecting project delivery and system performance :- ▪ Site surveys & records, financial budgets, deliverability within project time constraints ▪ Reference to standards and guidelines (i.e. Secured by Design, CPNI, NaCTSO) ▪ Prepare outline details of each system – typically: CCTV, IDS, PIDS, EACS, lighting, SMS or other control room systems etc. ▪ Control room human factors and ergonomics ▪ Consideration of financial implications of approach i.e. cost plan, risk appetite, total cost of ownership etc. ▪ Procurement methods, project risks, CDM regulations, planning (spatial) consents, stakeholder (including statutory) involvement ▪ Risk of failure of systems through the system life cycle, redundancy and resilience ▪ Maintenance aspects to provide continuity of service ▪ Mitigation techniques to prevent/reduce the impact of insider threats causing system disruption Ensure that L1 & L2 OR's are fulfilled together with client agreement in principle.

	Concept Design Refine and confirm operability of design options. Detailed Design Final definition of requirements : ▪ Drawings, schematics, specifications and layouts ▪ Consider connectivity and links to other building systems (i.e. electrical/HVAC etc.) ▪ Compliance with applicable BS, EN standards and guidelines (i.e. Home Office CAST, CPNI) ▪ Stakeholder sign off – design team, client, regulatory bodies, insurers. ▪ Resources & procurement – role of the quantity surveyors, contractors and suppliers ▪ Detailed programme and cost plan ▪ Adherence to CDM, occupational health & safety ▪ Compliance with legislative requirements i.e. DPA, DDA, FIA, HRA, Privacy Impact Assessment, PACE ▪ Preparation and alignment with general contract prelims/specific legal issues Contract Administration (Project) Management Ability to deliver projects from tender stage through to handover, typically : ▪ Manage the (security) contractor/stakeholder interface ▪ Contract administration e.g. pre-contract setup, factory acceptance testing (FAT), project management and cost control, snagging, handover, commissioning, witness testing, O&M manuals, training, maintenance, life cycle, auditing (benchmarking) Detailed scope not exhaustive, for example only: CCTV ▪ Standards & guidance e.g. BS EN 62676-1-1:2014, BS EN 62676-4:2015, CPNI Video analytics programme, Home Office Surveillance Code of Practice - 2013, BS 8418, client requirements, security inspectorates – National Security Inspectorate (NSI), Security Systems & Alarms & Inspection Board (SSAIB), Police (NPCC – Security Systems Policy 2015), Tempest, EMC directives, CDM, Privacy impact assessment ▪ Operational Requirements – Determination of Level 1 and Level 2 Operational Requirements, system grading to BS EN 62676 & CPNI standards & guidelines, respectively ▪ Cameras & Lenses – fixed, PTZ, camera metrics (field of view – object size vs. person screen height equivalent, use of 'heads' test control sheet – CAST, video test target, use of 3D modelling), dynamic range, shutter speeds, mountings,

	types of lenses and lens filters etc. ▪ System Infrastructure – Analogue & IP digital distribution, containment, multiplexing, radio, microwave, Laser, IP, fibre, copper based ▪ Telemetry and control systems (system types, system latency, consideration of primary, secondary & failover requirements for critical systems ▪ Control room layout/functionality ergonomics, environmental, lighting and human factors & failover scenarios ▪ Image Recording – Types of recording systems (Analogue, Digital, RAID, NAS, SAN, Distributed server etc.), impact of image digitisation and encoding/compression technology/artefacts, recording rates, archiving & retrieval etc. ▪ Image Display – Human factors, ergonomics, types of display, performance of display technology ▪ Evidence – Removal, effects of compression, storage, recording rates, factors affecting mass storage/removal ▪ Lighting – Types of lighting (Visible, IR etc.), colour rendering and temperature, background/foreground lighting, uniformity, life cycle of sources ▪ Integration into other systems - links to IAS/PIDS/AACS/Barriers/ARC/RVRC etc. ▪ Maintenance – Types (preventative/corrective), remote systems and stakeholder requirements (Police/Insurers) <u>IDS/PIDS</u> ▪ General – Risk assessment, system & environmental grading, protected area, impact of system operation on response levels (electronic and manned) ▪ Standards - BS EN 50131 series, insurance requirements, NSI, SSAIB, Police (NPCC – Security Systems Policy), CPNI ▪ Detection Types & Systems – Passive & Active Infra-red, Microwave, dual technology, acoustic, video, vibration, pressure, fibre etc. Effect of environment and other influences i.e. electrical noise etc. on false alarms and their prevention ▪ System Infrastructure – Analogue & digital distribution, containment, multiplexing, radio, IP, fibre, copper based, bus systems

	▪ Control and Indication Equipment (CIE) – Determination of system operation, alarm verification techniques (sequential, audio, video etc.), location of equipment and types of system and their operation ▪ System monitoring – Types (onsite/offsite), communications systems i.e. REDCARE, GSM, modem, IP, dual signalling transmission paths ▪ Integration into other systems - links to other systems i.e. FIRE/PIDS/EACS/Physical Barriers/alarm receiving centres (ARC)/remote video receiving centre (RVRC) etc. ▪ Maintenance – Types (preventative/corrective), remote systems and stakeholder requirements (Police/Insurers), management processes for false alarms/alerts and compliance with standards and guidance in relation to response times <u>EACS</u> ▪ General risk assessment - Determination of the level of security, definition of protected area, impact of system operation on response levels (electronic and manned), management of data, DDA/HSE/Failure modes ▪ Security grading ▪ Environmental consideration, access control point operation, system infrastructure & resilience ▪ Standards - BS EN 60839-11 series, insurance and building control requirements, NSI, SSAIB, CPNI ▪ Electronic Acceptance Device – Types of reader and electronic keys (magnetic strip, contactless chip, RFID, biometric, PIN etc.), effect of environmental affects and performance of technology types i.e. false accept & reject, effect of encryption etc. ▪ System Infrastructure - Analogue & digital distribution, containment, radio, IP, fibre, copper based, bus systems i.e. Weigand vs. encrypted protocols. ▪ Control Systems – Determination of system operation, types of system and the impact on operability (human factors) ▪ Electric Locking systems – types of devices and their physical capability to resist attack (motorized, solenoid, bolt, maglock, key etc.), failsafe/fail secure modes, interfacing with physical locks and fire evacuation systems. Understanding of fire regulation and building control requirements for evacuation and impact of 'lockdown'. ▪ System monitoring – Types (onsite/offsite), communications systems i.e. IP

	▪ Integration into other systems - links to FIRE/PIDS/Barriers/ARC/ etc. ▪ Maintenance – Types (preventative/corrective), stakeholder requirements (Police/Insurers) and compliance with standards & guidelines. <u>Integrated systems</u> ▪ References to Standards and Guidelines, NSI, SSAIB, Police (NPCC – Security Systems Policy 2015), Tempest, EMC, CDM, CPNI ▪ Determination of Level 1 & Level 2 Operational Requirements ▪ Integration into other systems and system redundancy/resilience i.e. UPS/duplication etc. ▪ Risks of delivery and procurement, software/hardware issues, legacy systems ▪ System Infrastructure – Distribution, containment, multiplexing, radio, IP, fibre, copper based ▪ Command and Control – Telemetry control, interface between systems (electronic hardware/software, protocols), user interface layout and human factors. ▪ Information Display – Human factors, types of display, performance of display technology ▪ Maintenance – Types (preventative/corrective), remote systems and stakeholder requirements (Police/Insurers)

CATEGORY D: CBRN

Introduction	CBRN candidates, although drawn potentially from diverse technical backgrounds (e.g. science, security engineering, general security adviser, etc), are expected to have knowledge, understanding, and experience in the following areas: • the effects of CBRN materials on people and the urban environment; • how to identify CBRN vulnerabilities in the urban environment; • sources of accurate CBRN threat information; • how to undertake a CBRN risk assessment that will inform the development of mitigation solutions and response strategies; • how conventional security measures, including mail-screening, can be optimised to reduce CBRN-specific vulnerabilities; • the basic principles of relevant CBRN protection technologies (e.g. filtration) and the effectiveness against the different classes of CBRN materials; • the basic principles of CBRN detection technologies (including their limitations) and their potential application to both security screening and to inform protection/mitigation strategies; and • the basic principles of CBRN emergency response procedures, including those provided by the emergency services. Prospective candidates, or those looking to re-grade their level of registration, should clearly evidence that they have attained a suitable level of competence against the above criteria, but also their (a) ability to effectively communicate (written and verbal briefing) with non-specialists and technical teams alike, and (b) know and understand the limitations of their own technical knowledge, and when to consult with more suitable experts. An academic qualification in a relevant CBRN discipline (e.g. chemistry) is not a pre-requisite for Technician Member grade but becomes increasingly desirable for Member and Principal Member grade.

Scope	General Operational Requirements (OR) – User Requirements Document. Ability to interpret, apply and develop threat and risk assessments and to develop solutions and response methodology. Hazards and their effects Chemical – Understand the range of potential hazards from toxic industrial chemicals through to chemical warfare agents. Demonstrate an understanding of the methods and level of difficulty associated with making these materials as well as the availability of precursors. Availability of toxic industrial chemicals. Understand a variety of dispersal mechanisms, improvised devices, explosive dissemination, spray release, pool release. Understand health effects and environmental impacts. Biological – Understand the range of pathogens and toxins which could pose a hazard. Understand the difference between toxins, bacteria and viruses. Understand the level of complexity associated with the different types of biological material and understand the range of methods which may be used to disperse the material. Understand health effects and environmental impacts. Radioactive –Understand the different types of radiation (alpha, beta, gamma and neutron) and the most commonly used radiological isotopes. Understand the potential methods for dissemination, dispersal devices, emplacement devices. Understand health effects (stochastic and deterministic) and environmental impact. Nuclear – Understand what fissile material is, understand criticality and the difference between nuclear and radiological events. Understand the immediate effects and the longer term impact of nuclear incidents. Understand the level of complexity of nuclear weapons development. Modelling – Understand what types of modelling are available for CBRN events, the limitations of the modelling and how modelling can help you understand the threat/hazard in indoor and outdoor environments. Mitigation Strategy: Detection Chemical – understand the laboratory and field based technologies for detection, and identification of chemical hazards. Understand the limitations and operational issues. Biological – understand the various technologies for detection and identification of biological materials and toxins. Understand the limitations of technology and the requirements for laboratory confirmation. Understand operational issues

	Radiological – understand the technology for detection of the different types of radiation and how a radio-isotope can be identified. Understand the limitations and the impact of background radiation. Understand operational issues. Networking – Understand the principles of networking detectors for detection/monitoring of an area. Understand limitations and operational issues. Stand-off and point detection – understand the differences, how they could be used and limitations <u>Mitigation Strategy: Protection</u> Mail Screening – Understanding and awareness of BSI PAS 97. Understands the "powder" screening methodologies, their limitations and the protective measures required. Understands the requirement of separate air space or ideally off-site location for any mail screening. Understanding of the limitations of technology in support of powder screening. Protective Equipment – understanding of Personal protective equipment and escape hoods and their limitations Type of ventilation – Understanding of different types of building ventilation system (natural, mechanical, hybrid), optimal location of air intakes, importance of zoning Protected Spaces – Understanding of options for providing protective spaces including pressurisation and filtration, understand how to trigger for use versus having them "ready" all the time Filtration – Understanding of different types of particulate filter and chemical filters. Understand limitations of protection and the increased power requirements for filtration, understand pressure drops, engineering issues <u>Mitigation Strategy: Response & Recovery</u> Understands key actions which should form the immediate response to CBRN incidents. Consideration of evacuation routes, shelter in place options, communications with staff and emergency services. Understanding of the emergency services response. Understand personal decontamination (wet and dry decontamination) Understanding of business continuity. Understanding of the contamination issues from a range of CBRN agents and what this means in terms of denial of access, decontamination process, role of Government Decontamination Service (GDS) communications with staff.		
	Technician Member	**Member**	**Principal Member**
Knowledge criteria	Basic understanding of types of CBRN hazards their effects. Basic knowledge of mitigation measures for all types of CBRN incidents or good knowledge for C, B or R/N events with a basic understanding of other types of CBRN event.	Good understanding of types of CBRN hazards and their effects. May have further expertise in one category of material. Basic knowledge of mitigation measures for all CBRN incidents	Good understanding of the types of CBRN hazards and their effects. Will additionally have deeper understanding of at least one category of threat materials. Good knowledge of mitigation measures for all types of CBRN incident. May have enhanced

		and enhanced knowledge for one of C, B or R/N events. Good understanding of one of the technical mitigation strategies (i.e. detection, protection or response & recovery).	knowledge on one of C, B or R/N mitigation measures. Good understanding of more than one of the technical mitigation strategies (i.e. detection, protection or response & recovery). May also have enhanced knowledge on one particular mitigation strategy.
		Further guidance on formal training/academic qualifications is outlined below 1. Candidates seeking Principal grade registration will need to demonstrate a breadth of knowledge across the spectrum of CBRN materials, as well as a deep level understanding in one or more of the category of CBRN threat materials. Therefore, for example, candidates with a degree in biology (or other relevant science) will be expected to demonstrate that they also have a good understanding of the other classes of CBRN materials, and that this knowledge should be at a level no less than that expected for Member grade candidates. 2. Candidates seeking to <u>solely</u> evidence formal 'NBC' training gained through the military (or similar), will be expected to demonstrate that they have augmented this formal training in recent years to understand the varying issues associated with CBRN in an urban/homeland security environment, either through additional formal CBRN training or via recent application of their knowledge in this same environment.	
Competence criteria	Can prepare OR documentation. Can provide basic advice on the type of impacts likely from CBRN incidents Can offer limited advice on mitigation strategies.	Can provide detailed advice on the type of impacts likely with CBRN incidents. Can offer basic advice across the range of mitigation strategies. Can offer detailed advice on one particular area of mitigation strategy.	Can provide detailed advice on the type of impacts likely with CBRN incidents Can offer detailed advice across a range of mitigation strategies. Will consider proportionality of advice (cost-benefit).

CATEGORY E: HOSTILE VEHICLE MITIGATION

Introduction	Candidates for RSES accreditation in the field of Hostile Vehicle Mitigation (HVM) will need to be able to demonstrate strengths in (at least) the following areas. A knowledge of crash testing to 68 and IWA 14.1. Ideally, candidates will have witnessed and crash test, to appreciate the magnitude of forces involved. This category specifically requires candidates to be able to show a practical understanding of the full range of crash tested Vehicle Security Barriers (VSB) products supplied by manufacturers and their site specific requirements; including the properties of different variants and foundation solutions. At Member and Principal Member grades, candidates should be able to deliver detail drawings and specifications showing PAS 69 / IWA14-2 compliant bollard and foundation setting out. This should also include an understanding of the factors involved in assessing a site to conduct a HVM survey, (i.e. all traversable routes) and the effects of topography on preparing a site specific Vehicle Dynamic Assessment (VDA). Candidates are expected to show applied knowledge (qualitative and quantitative) of the effects of the site and buried services on the choice of HVM product. They are also expected to understand the need to prepare an operational requirement OR1 and OR2 following consultation with key stakeholders. They will also appreciate when site constraints effect the choice of foundations and how working with other members of a design team, particularly the landscape architect and highways consultant. They will have knowledge of ground conditions and limitations imposed by the presence of utilities. This category is available at all three grades. At Technician Member grade, candidates will have knowledge and experience of the application of manufactures' crash tested product information carrying out tasks such as setting out measures to PAS 69/IWA 14.2. Candidates at Member level should, in a holistic security context, be able to apply knowledge of HVM and the implication and operation of vehicle access control points and how these systems need to be integrated into the access control and monitoring systems. At Principal Member grade, this knowledge and experience will be more extensive and will enable candidates to undertake foundation modifications through engineering calculations and conduct onsite checking of installation for sign-off compliance with PAS 68/69 and IWA 14.1 and IWA 14.2

Scope	**General** Level 1 Operational Requirement (OR1), User Requirement Document, Level 2 Operational Requirement (OR2) Ability to interpret, apply and develop threat and risk assessments **Type of Vehicle Borne Threat** 5 styles of vehicle borne IED threat – Parked, Penetrative, Encroachment, Deception and Duress, plus vehicle as a weapon against infrastructure and vehicle as a weapon against people. Single/multiple vehicles, layered attacks. Understanding composition of vehicle fleet, manoeuvrability, mass and speed, size and load capacity, modifications (structural, handling, cosmetic); **Type of Human threat** Number of attackers, skill of attacker (unskilled, knowledgeable, expert, state actor), hostile reconnaissance, armed or unarmed, theft, protest, climbing, cutting, burrowing, use of tools, use of vehicles to assist. **Site assessment** Topography, location, vulnerabilities, environment – climate, drainage, vehicle access- terrain, surface conditions, traffic calming, line of approach, vehicle dynamics assessment (acceleration, cornering, handling, look up tables, software analysis, vehicle approach route, rules of the road, swept path), site utilities and site specific issues, Stakeholders (site owners, staff, site operators, security, neighbours, local authorities etc.), effect on local traffic flow, site operation (search and screening, rejection lanes) , visitor and staff access, consequences of attack (alternative access, contingency planning), perimeter fencing (integration with VSB's), oversight, lighting , CCTV, Intruder detection, look and feel of perimeter barrier, vehicle access control points (VACP) and pedestrian access control points (PACP), security (guard force manning, training, control room), Security response (unarmed, armed, police, emergency services) **Barrier systems** Permanent, temporary, static, operational, retractable, manual, automatic, hydraulic, electric, site requirement (gate, blocker, bollard), operational requirement (OR2), specification, operational-frequency, speed, VACP (final denial, interlock), access arrangement – vehicle type, authorised vehicles, visitors, safety systems, manual override, location of control systems, operation of barrier, local, remote, Automatic Access Control, aesthetics, perimeter fence specification (height, material, topping, delay), hosting of perimeter intruder detection system (PID), access/egress points (gates, turnstiles, emergency egress), whole life costing, maintenance, servicing, warranty, ground conditions, environmental conditions (wind, climate, drainage), integration of measures. **Test and industry criteria and legal** National and international impact test standards, manual forced entry standards , HMG standards where applicable, relevant manufacturing standards for machinery, knowledge of applicable legislation (CE marking), Health and Safety legislation, working directives, Equality Act (Disability Discrimination Act), Operational Requirements, standard operating procedures. Road Traffic Regulation & Highways Acts, Anti-Terrorism Traffic Regulation Orders (ATTRO)

	Technician Member	Member	Principal Member
Knowledge criteria	Basic knowledge of specialist area Knowledge of test standards. Understanding of barrier classification.	In-depth knowledge of specialist area Able to demonstrate awareness of relationship of other physical security disciplines and their relevance to the project. Can demonstrate an understanding of dynamic impact its effect and the relationship to structural design (foundations). Awareness of design criteria relating to permanent and temporary vehicle security and perimeter barriers (wind loading, site conditions).	In-depth knowledge of specialist area and demonstrate a strong knowledge of other specialisms. Demonstrate an understanding of dynamic impact and its effects and the relationship to structural design (foundations). Awareness of design criteria relating to permanent and temporary vehicle security and perimeter barriers (wind loading, site conditions).

Competence criteria	Can demonstrate ability to work as member of project team – under supervision Able to identify potential systems against the identified threat. Can draft Operational Requirements. Able to prepare performance specifications	Can prepare detailed design from outline specification. Can deliver level 1 and level 2 Operational requirements. Provide technical review of design and deliver technical reports. Demonstrate a good understanding of national and international impact test standards for vehicle security barriers and associated standards for guidance and installation. Identify relevant test standards for the evaluation of perimeter security barriers and the reason for their choice. Can demonstrate project and risk management skills (small projects) Good interpersonal skills – able to communicate requirements to technical team. Undertake site surveys Able to develop standard operating procedures. Can demonstrate the need for servicing, maintenance and able to provide specification for contracts to be set up. Knowledge of relevant areas of legislation for the physical security barrier and associated security measures that might be utilized.	Able to deliver a detailed design from initial client requirement - demonstrate a broad portfolio of schemes - from concept to completion. Able to identify and respond to evolving requirements and challenges and develop appropriate measures – demonstrate lessons learned. Demonstrate the ability to interpret test data from dynamic impact tests, provide interpolation where appropriate, in order to deliver a structural foundation for site specific solutions. Demonstrate the relevance of National, International and Government test standards and their effect on the choice of physical security measure(s). Have strong interpersonal skills demonstrating good project management and team leader skills. Demonstrate the ability to communicate to stakeholders, non-technical and technical teams, a clear and concise message with the relevant technical content, to enable decisions to be taken.

CATEGORY F: PROTECTION AGAINST FORCED ENTRY

Introduction	Candidates for registration in the field of Protection against Forced Entry will need to be able to demonstrate that they can undertake a site security survey and assess topography, location, vulnerabilities, environmental conditions, site utilities and site specific physical security issues. They should be able to assess construction materials used to form walls, floors and roofs, glazing and framing assessment, door locks and materials. Candidates will be able to take an operational requirement (OR) document and provide a suitable level of physical protection using fences and building fabric. This protection might be for resistance to both criminal and terrorist attack and be specified cognisant of the type and time of response. Candidates will have knowledge and experience of a range of attack methodologies, as defined by both publicly available and government test standards, and appropriate applicability of the standards, to the project needs and that of specific materials, i.e. doors, windows, walls, hatches, barsets and grills (including their locking systems). Candidates will be able to demonstrate an understanding of how to specify intrusion detection systems to ensure detection occurs at the earliest opportunity. Candidates at Member grade should be able to demonstrate, by knowledge and experience, that they are able to specify/provide solutions that mitigate the designated risks, by strengthening the building fabric, creating multiple approved security layers (walls, portals, floors, locks) between the perimeter and the protected assets. At Principal Member grade, this knowledge and experience will be more extensive and will enable candidates to adapt or develop new materials/mitigation measures and deal with new attack weapons or changing threat scenarios. At this grade, candidates will also be able to engage other security specialists in technical discussions and advise senior non-technical personnel on complex technical issues.

CATEGORY G: EXPLOSIVES AND WEAPONS SEARCH AND DETECTION

Introduction	Candidates for registration in this category must demonstrate experience and vision in delivering search and screening measures, and balancing effectiveness and efficiency, while addressing other client priorities such as aesthetics and visitor experience. In common with other aspects of security, specifying and delivering appropriate and effective search and screening measures involves far more than just choice of equipment. Robust application of an operational requirements methodology is essential to understanding the needs and constraints of the client organisation/site – for both current and potential future needs. This will, in turn, enable appropriate search and screening measures to be identified, specified, procured and delivered, and done so in a way that complements other security measures. Key considerations typically include: • understanding detection priorities and throughput requirements; • choice of technologies and techniques; • development of policies, procedures and processes; • available space, how it can best be used, and supporting infrastructure requirements; and • ensuring staff are suitably trained and motivated. This category is available at all three grades.

Scope	General Operational Requirements (OR level 2) – User Requirement Document. Ability to interpret, apply and develop threat and risk assessments. Explosives & weapons Military, commercial, improvised explosives. Explosive devices and typical component parts. Weapons including firearms (including reactivated and improvised), ammunition and bladed weapons. Science and technology of detection Characteristic features/attributes/signatures of weapons, explosives, explosive devices that may enable detection. Underpinning chemistry, physics and statistics of detection. Technological approaches to detection. Canine search and detection. Weapon and blast effects Basic awareness and knowledge of weapon and blast effects with regard to safe design of explosives and weapons screening processes and facilities. Design and implementation of search and detection solutions Modes of delivery of explosives and weapons threats. Commercially available detection equipment including its capabilities and limitations. Other aspects of protective security relevant to delivering successful search, detection and screening. Systems engineering as relevant to specifying and delivering a search and detection solution, including: ▪ equipment selection and integration ▪ process design ▪ facility design / layout ▪ ergonomic considerations ▪ human factors (including training, staff motivation) ▪ consideration of whole life costs (including equipment, maintenance and staffing). Health and safety considerations. Operating procedures and emergency responses (specific to search, detection and screening activity and integration with wider procedures / responses). Search and detection solutions for chemical, biological, radiological and nuclear (CBRN) materials and devices Basic knowledge of CBRN materials and devices and approaches to their detection. ▪ *NB: Whilst more comprehensive CBRN detection and screening requirements should be addressed by Specialist CBRN Security Advisers, many explosives and weapons detection measures will offer some, albeit limited, CBRN capability.*

	Technician Member	Member	Principal Member
Knowledge criteria	Awareness of all aspects of explosives and weapons search and detection, as listed under *Scope* above. Knowledge of explosives and weapons threats and their potentially detectable attributes. Basic knowledge of all aspects of *Design and implementation of search and detection solutions*, as listed under *Scope* above, combined with detailed knowledge of more basic search and detection solutions.	Knowledge, supported by practical experience, of *Design and implementation of search and detection solutions*, as listed under *Scope* above. Sound general knowledge of all other aspects of explosives and weapons search and detection.	In-depth knowledge, supported by extensive experience, of *Design and implementation of search and detection solutions*, as listed under *Scope* above. In-depth knowledge of many other aspects of explosives and weapons search and detection. Knowledge of the remaining aspects. Knowledge of other relevant aspects of physical protective security, including access control, weapon and blast effects, and CBRN.
Competence criteria	Can contribute to design and implementation of basic solutions working under supervision as part of a team.	Can produce specifications for, and implement, basic solutions in response to clearly documented Operational Requirements.	Can demonstrate a portfolio of varied and more complex screening solutions, from concept to completion, which are fully integrated with wider protective security capability. Can develop new approaches and responses to new situations. Can demonstrate lessons learned, and can pre-empt problems. Can engage technical and non-technical colleagues in complex discussions. Can produce outline designs Substantial interpersonal skills. Can produce high quality reports, including OR documentation. Can engage security professionals in technical discussion.

CATEGORY H: FORCE PROTECTION ENGINEERING SPECIFIC CRITERIA

Introduction	Candidates for registration in the field of Force Protection Engineering will need to be able to demonstrate that they can take a user requirement document, apply risk assessment techniques and provide a suitable level of protection for the period required. This protection might be for an expeditionary force, aid programme, disaster relief, necessary infrastructure/logistics operation or some other purpose, but is likely to be outside the UK and may well be in a hostile environment. It will involve some flexibility to deal with a possibly changing threat and also involve experience in prioritising actions in the light of immediate requirements and limited resources. Candidates are likely to have knowledge and experience of a range of weapons effects, including small arms, rockets, mortars, explosive devices, CBRN, and vehicles. They will also have experience in liaising with national and local authorities and other security specialists with local experience. They must be capable of operating in foreign cultures/languages and reporting back up the management chain as required. This category is available at Member and Principal grades only. Candidates at Member grade should be able to demonstrate, by knowledge and experience, that they are able to specify/provide solutions that mitigate the designated risks using available resources to a level that is acceptable to the senior personnel responsible. At Principal Member grade, this knowledge and experience will be more extensive and will enable candidates to adapt or develop new materials/mitigation measures and deal with new weapons or changing threat scenarios. At this level, candidates will be able to engage other security specialists in technical discussions and advise senior non-technical personnel on complex technical issues.

Scope	General Operational Requirements (OR level 1) – User Requirement Document Ability to conduct, interpret, apply and develop the engineering requirements from the User Requirement Document Sufficient awareness of weapons effects including blast, fragmentation, heat/incendiary and earth shock to be able to understand the engineering effects on a structure Types of asset Built environment including expeditionary structures with short design lives (up to 5 years) Existing and new buildings/installations/centres in the public and private sectors Collective protection from CBRN threats Infrastructure – e.g. communications, utilities, ports, airports, road and rail networks Critical National Infrastructure (CNI) Stadia, shopping malls, hospitals, government buildings, financial centres, residential centres, iconic sites Expeditionary Engineering Force Protection Unstable regimes e.g. Kosovo, Iraq, Afghanistan Trials for developing solutions (Trials Director for Principal) Multinational, multi-agency delivery of security projects within campaign plan Embassies and consulates, overseas offices and stations etc. Mode Proactive/active – threat mitigation measures and precautionary protection Reactive – disasters/response to crises and events that threaten business continuity Pre-emptive – consequence planning/preventive measures Appropriate responses that match available resources to the threat and the level of risk acceptable to the commander/CEO Roles Identify and prioritise requirements for action – accommodation, food, water, power, infrastructure Planning and logistics Liaison with national and local authorities and other security specialists Adapt existing/available materials and resources to deliver appropriate solutions (Principal) Interface and coordinate with business continuity planners

	Member	Principal Member
Knowledge criteria	The following in reasonable breadth and depth: Risk assessment methods Knowledge of weapons effects Business processes/practices (understanding value). Security processes/practices Impact analysis (critical dependency) Tools (risk scoring) and their limitations Mitigation measures (cost/benefit analysis) Relevant contracts, standards & guidelines Understand technical aspects of security measures/proposals	The following in substantial breadth & depth: Risk assessment methods Knowledge of weapons effects Business processes/practices (understanding value). Security processes/practices Impact analysis (critical dependency) Tools (risk scoring) Mitigation measures (cost/benefit analysis) Relevant contracts, standards & guidelines Can engage security professionals in technical discussion
Competence criteria	Application of threat and risk assessment theory (see above) to a targeted range of real situations Can apply existing approaches and responses to situations Good communication skills Can produce standard reports including OR documentation.	Application of threat and risk assessment theory (see above) to a wide range of real situations. Can develop new approaches and responses to new situations. Can engage other security specialists in technical discussion. Can advise senior non-technical personnel on complex technical issues. Can produce high quality reports including OR documentation.

CATEGORY I: DIGITAL BUILT ENVIRONMENT SPECIFIC CRITERIA

Introduction

Candidates for registration in the field of Digital Built Environment will need a broad understanding of all aspects of digital engineering relating to the built environment and a detailed understanding of the associated security implications.

Candidates are likely to have detailed experience of one of:

- Digital modelling of the built environment and the management of information.
- Designing, installation or maintenance of digital building systems to support the built environment.

They will also be able to demonstrate an understanding, to the appropriate level, of the threats to such digital models and systems, and will be able to explain the vulnerabilities and risks that these therefore present to the security of the built environment.

Candidates are expected to understand the interaction between physical, human and digital ('Cyber') security and be able to describe these using the language of information security assurance.

Successful candidates will be able to bridge the gap between the logical, virtual worlds of information security and the tangible, physical world of construction and operation in the built environment.

The category is available at Technician Member, Member and Principal Member grades. Technician Members will typically be employed and experienced in applying security to an existing modelling or design environment. Members will be involved in the management of such environments and will contribute to policy development. Principal Members will be primarily involved at the policy level, helping to influence information assurance approaches and determine the shape of the future digital built environment.

Scope	General Understanding and advising on the interaction between personnel, process, physical and cyber security domains in the protection of the built environment, built assets, their occupiers and/or users, and the services provided. Understanding of the different security roles and domains, and the need for adoption of a security-minded culture. Ability to work in an interdisciplinary environment to identify risks and technology, process or human factors and solutions. Risk management Understanding of the potential impact of threats and vulnerabilities on digital engineering, built asset systems (both buildings and infrastructure), control systems, asset management systems and the digital built environment. Ability to survey, assess relevance and communicate the emerging threats to the design and operation of the built environment across the lifecycle of a built asset. Undertaking risk assessments, and formulating, collating and assessing potential countermeasures or controls to manage and minimise risks. Policy development and management Ability to interpret, apply and develop threat and risk assessments, to develop security strategy covering people, process, physical and technical aspects, and to develop solutions and response methodology. Developing, maintaining and reviewing the security documents required for implementation of PAS 1192-5 or other relevant standards or guidance documents. Undertaking audits of documentation, policies, processes and procedures to identify gaps and assess compliance with security strategies and plans. Information management Understanding of the issues related to the governance and management of data and information, the need to protect sensitive information and the issues associated with data aggregation and the use/publication of open data. Systems engineering Understanding of the inter-relationships between systems in the digital built environment and the need for a security-minded approach to their design, implementation, operation and maintenance. Understanding of the process of monitoring cyberspace for changes in the risk environment.

	Technician Member	Member	Principal Member
Knowledge criteria	Basic knowledge of risks and their impact and potential ways of mitigating them Basic knowledge of information management and systems engineering	Good knowledge of risks and their impact and potential ways of mitigating them Basic knowledge of policy development and management Good knowledge of information management and systems engineering	Substantial knowledge of risks and their impact and potential ways of mitigating them Good knowledge of policy development and management across multiple sectors Substantial knowledge of information management and/or systems engineering, across multiple sectors
Competence criteria	Detailed assessment, reporting and development of solutions in specific areas covered by the scope	Detailed assessment of specific areas and development of solutions, accompanied by a broader general understanding. Demonstrates competence on a range of moderately-sized and complex projects involving most aspects included in the scope.	General strategic and detailed assessment and development of solutions. Demonstrates competence on a full range of relevant projects and systems involving the topics covered by the full scope.

CATEGORY J: PERSONNEL SECURITY (INSIDER THREAT)

Introduction	Candidates for registration in the field of Personnel Security (Insider Threat) will need to be able to demonstrate strengths in particular areas, e.g., personnel security risk assessment, insider threat monitoring and security culture. This specialist category specifically requires candidates to be able to show practical understanding of holistic protective security and of how insider risk, at both strategic and operational levels, can be reduced through targeted integration of personnel, physical and cyber security measures. Candidates are expected to show applied knowledge from relevant sources i.e. regulators (e.g. the Information Commissioner's Office (ICO)), security authorities (e.g. CPNI), professional institutes (e.g. CIPD) and academic institutions. At Principal level, candidates will be able to show relevant experience in helping senior leadership teams recognise and understand their organisation's specific vulnerabilities to insider threat; recommend an action plan which may form a programme which helps the organisation reduce its strategic exposure to high risk behaviours from its people; and experience in helping organisations apply those measures as part of a programme of strategic improvement and risk reduction. At Member grade, candidates will be able to show relevant experience in helping organisations recognise their specific vulnerabilities to insider threat; identify the broad elements in an action plan to reduce their strategic exposure to high risk behaviours from insiders; and experience in helping organisations apply those measures as part of an holistic programme. Candidates need to demonstrate the application of their specialist knowledge and professional expertise in Personnel Security (Insider Threat) as set out below and through their specialist qualifications. Candidates are not required to demonstrate engineering, scientific or technical competences, commercial ability, or knowledge in sustainable development and health, safety and welfare.

Scope	<u>General</u> Show understanding of holistic protective security and how vulnerabilities can be reduced by integrated personnel, physical and cyber security measures. <u>Insider Threat</u> Demonstrate knowledge of types of insider threats – Unauthorised disclosure, process corruption, facilitation of third party access, physical, electronic or IT sabotage. Demonstrate knowledge of insider threat actors (e.g. terrorist, criminal, hostile foreign intelligence service (HFIS), commercial competitors, single issue groups, etc.), types of behaviour (e.g. volunteer/self-initiated, exploited/recruited, deliberate), motivations (e.g. financial gain, ideology, desire for recognition, loyalty, revenge), and methods used by hostiles (e.g. social engineering, manipulation, blackmail, honey-traps, etc.). Demonstrate knowledge of insider demographics and types of employee (permanent/contractor/remote worker). Demonstrate knowledge of relationships between insider motivations and type of insider incidents. Demonstrate knowledge of individual (personality traits, lifestyle/circumstantial vulnerabilities, workplace behaviours) and organisational level (management, audit, security culture, pre-employment screening, communication, risk awareness, corporate governance) factors associated with insider activity. Show understanding of non-malicious (both witting and unwitting) insider acts and the organisational enabling factors that enable them. Demonstrate knowledge of a range of insider case histories in order to be able to illustrate characteristics of insiders and insider acts. <u>Risk Assessment and Management</u> Demonstrate ability to develop, interpret and apply personnel security risk assessments at organisation, group and role level. Demonstrate knowledge of holistic management of employee risk principles and application within organisations. <u>Principles of Insider Risk Mitigation</u> Screening – What procedures to use for assessing threat and vulnerability associated with job candidates and current employees (staff), How to identify assess and resolve suspicions or anomalous behaviour. Shaping – How to establish organisational environments that deter, detect and disrupt insider threats.

	<u>Pre-employment</u> Demonstrate knowledge of pre-employment screening as an effective protective security measure to assess the reliability and integrity of a candidate. Demonstrate knowledge of the pre-employment checks (verifying identity, the right to work, confirming employment history & qualifications, verifying criminal records) which should form part of a pre-employment screening process. Show understanding of the critical importance of correct identity verification and the tools available to achieve this. Demonstrate knowledge of security screening methodologies and standards including BS7858:2012, national security vetting & HMG Baseline Personnel Security Standard, use of media screening, document verification. Show understanding of the methods, benefits and risks of pre-employment psychological evaluation and profiling. Show understanding of how pre-employment screening complies with relevant legislation. <u>On-going Personnel Security</u> Demonstrate knowledge of personnel security measures to mitigate the threat of insider acts from existing staff: identifying change, access controls, security passes and access privileges, management practices, manipulation, protective monitoring (including relevant legislation), whistleblowing and mechanisms for reporting concerns, and robust leavers' policy/process. Show understanding of the concept of security culture and demonstrate knowledge of the ways it can be assessed and the mechanisms by which it can be changed as part of an organisation's insider risk mitigation strategy. Demonstrate knowledge of how appropriate induction and continuous awareness training of employees can contribute to an organisation's insider risk mitigation strategy for both malicious and non-malicious insiders. Show understanding of social engineering mitigation methodology and demonstrate knowledge of behavioural methods that can be used to promote compliance with an organisation's security culture. Demonstrate knowledge of personnel security measures to mitigate the threat of insider acts from staff who work remotely. Demonstrate knowledge of personnel security measures to mitigate the threat of insider acts from staff who are contractors or who have access to an organisations assets through the supply chain. <u>Resolving Suspicions & Disclosure</u> Demonstrate knowledge of employee assurance mechanisms and investigative procedures and their use as resources for managing employee risk. Show understanding of the potential impact to businesses of employee –related information disclosed by the security authorities and demonstrate knowledge of the correct procedures for such disclosure consistent with employment law and the management of risk.

	Technician Member	Member	Principal Member
Knowledge criteria	Awareness of all aspects of relevant personnel security policies, procedures, processes and current legislation (including employment law, employee relations, recruitment, vetting, performance management and dismissal).	Demonstrate knowledge, supported by practical experience, of assessing, recommending and/or implementing personnel security mitigation measures as listed in the scope above. Demonstrate in depth knowledge of at least one mechanism/tool for addressing specific personnel security issues (e.g. security culture, employee assurance.) Basic project management.	Demonstrate in depth knowledge of all personnel security mitigation measures listed above supported by extensive experience of personnel security solutions, as listed under *Scope* above. Complex project management.
Competence criteria	Can lead the delivery of personnel security risk assessments at group and role level and for simple organisations. Can audit an organisation's pre-employment screening and vetting processes and make recommendations with regard to compliance with good practice. Can audit an organisation's ongoing personnel security processes and make recommendations with regard to compliance with good practice. Interpersonal skills. Can produce accurate and concise factual reports.	Can lead the delivery of personnel security risk assessments at organisation, group and role level and for any organisation. As part of a wider insider risk mitigation programme, can lead the delivery of specific work packages within their knowledge criteria (e.g. security culture, employee assurance, workplace behaviours and employee vigilance). Well-developed interpersonal skills. Can produce accurate reports analysing complex personnel security issues.	Can engage with organisations at senior level to advise on development of a comprehensive, risk-based, insider risk mitigation strategy and can advise on its implementation. Can advise on security by design as part of business process change. Can demonstrate a portfolio of personnel security projects, which are fully integrated with wider protective security capability. Can develop new approaches and responses to new situations. Can demonstrate lessons learned, and can pre-empt problems. Can engage technical and non-technical colleagues in complex discussions. Substantial interpersonal skills. Can produce high quality reports including analysis, assessment and gap analysis and make appropriate recommendations.

CATEGORY K: PERSONNEL SECURITY (HUMAN FACTOR)

Introduction	This category will be available shortly. Candidates will not be required to demonstrate engineering technical knowledge or expertise and need only demonstrate the specialist competence as set out in Annex C. Please contact registers@ice.org.uk for further details.

Annex D

Acronyms

AACS	Automatic Access Control system
ALO	Architect Liaison Officer
ARC	Alarm Receiving Centre
ASC	Association of Security Principals
ASIS	(formerly) American Society of Industrial Security
CBRN	Chemical, Biological, Radioactive, Nuclear
CCTV	Closed Circuit Television
CPO	Crime Prevention Officer
CTC	Counter Terrorism Cleared
CTSA	Counter Terrorist Security Member
DADA	Deadly & Determined Attack
DV	Developed Vetting
EOD	Explosive Ordnance Disposal
Hazmat	Hazardous Materials
HPA	Health Protection Agency
IAS	Intruder Alarm System
IDS	Intruder Detection System
IEDD	Improvised Explosive Device Disposal
IIS	International Institute of Security
List X	Companies classified by MOD
OR	Operational Requirement (Govt. spec.)
PIDS	Perimeter Intruder Detection System
RA	Risk Assessment
RPG	Rocket Propelled Grenade
SC	Security cleared
SIA	Security Industry Authority
TA	Threat Assessment
TIC	Toxic Industrial Chemicals
TSI	The Security Institute
DPA	Data Protection Act
DDA	Disability Discrimination Act
FIA	Freedom of Information Act
HRA	Human Rights Act
CDM	Construction Design Management
EMC	Electro Magnetic Compatibility
HVAC	Heating, Ventilation Air Conditioning
RAID	Redundant Array of Independent Disks
RVRC	Remove Video Receiving Centre
ATS	Automatic Transmission System
FAT	Factory Acceptance Testing
UPS	Uninterruptible Power Supply
ACPO	Association of Chief Police Officers
SBD	Secured by Design
PTZ	Pan Tilt and Zoom
IP	Internet Protocol
GSM	Global System for Mobile communication
RFID	Radio Frequency Identification Device
PIN	Personal Identification Number
BS	British Standard
EN	European Norm
O&M	Operation and Maintenance
AMS	Alarm Management System

Annex E Detailed Guidance

E1 Initial enquiries and expressions of interest

Initial Enquiries

Should you require assistance with your eligibility to apply for the RSES, please complete an RSES Enquiry form. With reference to the RSES guidance document at www.ice.org.uk/rses, you will need to prepare a 300 – 500 word statement. This should include your academic and professional qualifications, together with your current employment responsibilities and demonstrate your experience and technical expertise as a security practitioner in support of your preferred category and grade. Although you may be asked to supply further details, you are not required to submit authenticated copies of academic qualifications at this stage.

When complete, please forward your documents to the Professionalism and Registers Executive at registers@ice.org.uk. You will then receive feedback on your eligibility to apply. Should you be eligible, your route to registration will be one of three options outlined in 1.9 above.

Expression of Interest

Once you have received feedback, and if you are eligible to apply to the RSES, the Professionalism and Registers Executive may assist with arranging a sponsor to support you with your application.

If you are not professionally qualified, and do not possess the relevant academic base for the grade you wish to apply for, you may be advised to apply via the Technical Report Route (TRR). Further details on the TRR (link) are available.

You are required to submit an ICE 3920 Expression of Interest form which is countersigned by your sponsor, together with a brief CV and authenticated copies of any academic qualifications you have gained.

Your CV at this stage should be no more than 1000 words. It should provide a chronological review of your career and indicate your role and responsibilities held in various projects and/or activities with which you have been associated.

Certified English translations of academic qualifications should also be provided where applicable. Advice on authentication and the documentation to submit is available on the ICE website. Please note we may need to contact your university/college or professional body to verify the authenticity of your academic qualification(s). If any qualification is identified as fraudulent the application will be rejected.

Once your Expression of Interest has been has been acknowledged, your sponsor will be required to verify your identity (i.e. Passport/Drivers Licence) and current address (i.e. bank statement/utility bill).

Once verification has been received, you will have access to the RSES website and Continuing Professional Development (CPD) events hosted by the RSES.

E2 Application process

When the Expression of Interest process has been completed, the application for registration is in two parts. It requires you to:

- submit an application and associated documentation
- attend an interview with two appointed assessors

E3 Part 1: Application and associated documents

You will need to submit in hard copy, and not electronically, the following documentation:

- Application form
- Sponsor's statement
- Detailed CV
- Criminal convictions statement. This is to be submitted in a sealed envelope marked *Private and Confidential* for the attention of CPNI
- Two character references
- CPD record
- Assessment reports (see E8 below)
- Fee if applicable, details of anything that may affect your performance at assessment

All relevant forms to be completed are available at ice.org.uk/rses.

Security-mindedness and security clearance

You should consider whether information in your application should be omitted or reduced in its level of detail due to security reasons. However, there's no reason why this should detract from the quality of your evidence. If your application is affected by security issues, you should consider the following suggestions:

Make the evidence non-site specific – for example don't state that the facility was on the Sellafield site or on the Hinkley site or that the asset serves a critical function to the site or country, or is or was vulnerable to various threats.

Where applicable:

- Don't state building numbers or names – it's sufficient to say 'nuclear facility' or 'nuclear store'
- Remove site and building names from drawings or snapshots of models
- Don't include photographs or other images which reveal the location of buildings and facilities
- Avoid stating, or showing in drawings or extracts from models, technical details (such as wall thickness) which may reveal security-sensitive information

If you work on a security-sensitive project, we recommend that your organisation's information security manager (and also the asset owner's/client's) reads the evidence you are providing and approves the content before submission.

Should you consider that the evidence you provide needs to be specific please contact registers@ice.org.uk for further guidance.

E4 Sponsorship

To be eligible to submit a full application, the RSES requires that you are sponsored by a current registrant at the same grade or higher to the one you wish to apply for.

Sponsors may also act as mentors to candidates. The role of the sponsor is to identify which aspects of competence will form the basis for demonstrating the relevant attributes, to approve your submission and prepare you for interview. Your sponsor has a duty to act as a mentor during your submission process.

Your sponsor should know you well and be convinced, through direct experience, that you are a fit and proper person to be admitted to the register. In addition to completing the sponsor's statement, your sponsor should sign the application form and have read and signed the submitted reports.

E4.2 The scope of your sponsor's involvement should extend to constructive criticism of your reports, advice on your presentation and arrangement of practice interviews.

E4.3 Sponsors are requested to return the sponsor's statement as part of Stage 1 of the application process.

E5 Criminal conviction statement

Completion of the criminal conviction statement is a declaration of any matter which may be of relevance including any criminal conviction(s) you may have.

The form should be placed in a sealed envelope marked with your name and included with your application. Please note that any information provided will be treated in strict confidence.

E6 Character references

Two character references must be submitted using the character reference form e to provide information on the referee's connection with you and the specific skills and personal characteristics you have that they are endorsing.

E7 Continuing Professional Development

Detailed guidance on CPD requirements are set out in Section 4 of this document. Of particular interest will be your CPD activity relating to RSES matters.

E8 The assessment reports

Your reports are a vehicle for you to demonstrate how you've achieved the relevant criteria for the relevant category of application as set out in Appendix A. They should be your own work and presented in an ordered manner.

Your reports need to be approved and signed by your sponsor prior to submission.

E8.1

The grade of registration that you are applying for will determine the documents required as follows:

Grade	Experience Report	Project Report
Technician Member	1000 Words	Not required
Member	1000 Words	1000 Words
Principal Member	2000 Words	2000 Words

E8.2

Your experience report should describe the structured training and experience you have gained, including the tasks which you undertook. It must not be a mere inventory, although it should set out the development of your career and the precise positions you have occupied. It is essential that you emphasise your personal experience and the degree of responsibility assigned to you for each attribute.

You should give an indication of the size and financial value of the work undertaken.

E8.3

If you are applying for registration at Member or Principal Member grade, the project report should demonstrate your competence against the criteria set out in Annex C of this guidance document. It should put particular emphasis on one or two projects in which you played a major part.

Where relevant, you should also describe how you took a lead in some or all of the elements of the project/s. You must clearly indicate your role in any relevant aspects of the project/s you have worked on by giving the background to the important decisions you were responsible for, or made a significant contribution to. You should include the problems you met, and occasions when you gained unusual or extensive experience and learned valuable lessons.

You must show where you've exercised independent judgement – as a security engineer or specialist and a practising professional.

In relation to the project report's appendices: numerical analyses, cost data, drawings or other relevant additional documentation may be included as appendices to support the content of your reports. They are not included in the word count.

Your appendices should include no more than:

- Three A3 drawings
- Twelve A4 sides of additional information, including any relevant calculations

E8.4
If you are not professionally qualified, you should also demonstrate in your reports how you have met the generic engineering attributes in Annex B.

The application documents will be checked by the ICE Professionalism and Registers Executive. Candidates will be advised whether or not their application is complete and can proceed to interview.

If your Stage 1 application is approved, you will be invited to interview (Stage 2).
Please note that with the exception of your character references and criminal convictions statement, three copies of your application must be submitted **in hard copy only**.

E9 Part 2: The interview

E9.1
Interviews will be arranged at a date, time and location mutually convenient to both you and your assessors.

E9.2
You will be given approximately four weeks' notice for your interview date and the names of your assessors. If, on being notified of your assessors' details, you find that you personally know them, or feel there may be a conflict of interest, you should advise the ICE Professionalism and Registers Executive immediately via registers@ice.org.uk. Assessors are similarly advised to notify any conflicts of interest.

E9.3
You may postpone your interview if three weeks' notice is given.

E9.4
You will be interviewed by two assessors. Each assessor will be an experienced registrant and at least one will be matched to your assessment category.

E9.5
Assessors will seek to confirm that the evidence of competence that you have provided meets the requirements of Annex C and is supported by your responses to their questioning. If you have not demonstrated sufficient evidence of a particular criterion, assessors may frame specific questions to try to draw out your knowledge and experience in that area. However, it is your responsibility to demonstrate the achievement of the criteria as well as that of the assessors to identify if you possess them. This requires considerable communication skill on your part, both in the compilation of the reports and in discussion. If you are not professionally qualified, you will also have to demonstrate that you have met the attributes set out in Annex B.

E9.6
If you are applying for registration at Member or Principal grades, a 15 minute presentation is required at the start of the interview. It should be based on the project report and expand upon, rather than repeat, the information already given to your assessors.

Your presentation will be delivered opposite the assessors at a table. You may use visual aids such as flip portfolios, no larger than A3, to illustrate the presentation.

Whilst the use of laptop computers is permitted, experience has shown that you will need to plan the practicalities of your presentation with care.

E9.7
If you are professionally qualified, the presentation and interview will last for 60 minutes. If you are not professionally qualified, you will be given an additional 30 minutes to allow time to demonstrate the generic engineering attributes in Annex B. Although Technician Member grade candidates do not give a presentation interviews will also last for 60 minutes or 90 minutes as appropriate.

E10 Assessment results

E10.1
You will be advised by letter, within six weeks from the date of your interview, of the assessor's decision based on the evidence you have provided in your written submission and at interview.

E10.2
Should your assessment result in an overall failure, you will be provided with an indication of where your submission was satisfactory as well as the reasons for failure.

E10.3
If you have not demonstrated the knowledge and experience required for the applied grade you may be offered entry onto the register at a lower grade. However, you must have clearly demonstrated to the assessors the required attributes at the lower grade.

The award of a lower grade is not a default position of you failing to achieve the criteria for a certain grade. It is by exception and the examiners will use this exception where your knowledge, skills, performance and experience fall within the broad scope of the relevant grade.

In both situations of either failing to achieve a grade or being awarded a lower grade, you will be advised of the steps that should be followed before re-applying. You are advised to discuss this with your sponsor. This should help you prepare a strategy for any future application.

You must apply at the grade that you, and your sponsor, deem achievable.

E10.5
There is a right of appeal in cases of perceived error in process or for unforeseen events. Appeals are only accepted if received within two months from the date of the failure letter. For details, contact registers@ice.org.uk

E10.6
Should you be admitted at either Member or Principal Grade, your category of admittance will be listed on the RSES Company Competence List (link). You will be invited to apply for up to four additional primary and secondary categories.
See Section 7, page 9, for further details.

Annex F Summary Eligibility Criteria and Requirements

SECURITY ENGINEERS & SPECIALISTS			
Item	**Technician Member**	**Member**	**Principal Member**
Academic base	Relevant HNC or equivalent*	Relevant BSc or equivalent*	Relevant Master's degree or equivalent*
Generic competence	Technician or equivalent level attributes (see Annex B).	Incorporated or equivalent level attributes (see Annex B).	Chartered or equivalent level attributes (see Annex B).
Indicative experience	Necessary and sufficient experience on relevant work at EngTech level of responsibility or equivalent.	Necessary and sufficient experience at IEng level of responsibility or equivalent in relevant specialism.	Necessary and sufficient experience at CEng level of responsibility or equivalent in relevant specialism.
Specialist competence	Technician or equivalent level (see Annex C).	Incorporated or equivalent level (see Annex C).	Chartered or equivalent level (see Annex C).
Submission and assessment	i) 1000 word experience report, including academic and professional record ii) CPD plans & records for last 2 years iii) Interview	i) Summary of academic and professional record ii) 1000 word experience report iii) 1000 word project report iv) CPD plans & records for last 3 years v) Interview, including presentation of project report	i) Summary of academic and professional record ii) 2000 word experience report iii) 2000 word project report iv) CPD plans & records for last 4 years v) Interview, including presentation of project report
Post-registration CPD	To be reviewed biennially	To be reviewed biennially	To be reviewed biennially

Note *

1. The academic base is expressed in terms recognisable to engineering professional institutions for the levels of Engineering Technician, Incorporated Engineer and Chartered Engineer. This is an indicative level of academic knowledge.

2. The absence of a specific academic qualification does not preclude an individual from qualifying at that level within the Register. Please refer to RGN15, RSES TRR, available at ice.org.uk/rses. Alternatively, engineering professional institutions have mechanisms in place, as part of their membership policy, to accommodate such individuals through processes involving an academic review.

3. Register candidates without a recognisable professional qualification, and without the formal academic qualification level, are encouraged to contact an appropriate professional institution in the first instance.

4. Qualifications such as ASIS and IIS should be considered alongside the common criteria.

RSES Guidance

Institution of Civil Engineers

CPNI
Centre for the Protection of National Infrastructure

ice
Institution of Civil Engineers

ICE vision

Civil engineers at the heart of society, delivering sustainable development through knowledge, skills and professional expertise.

Core purpose

- To develop and qualify professionals engaged in civil engineering
- To exchange knowledge and best practice for the creation of a sustainable and built environment
- To promote our contribution to society worldwide

Diversity statement

As a membership organisation and an employer, we value diversity and inclusion - a foundation for great engineering achievement

Institution of Civil Engineers
One Great George Street
Westminster
London SW1P 3AA

t +44 (0)20 7665 2192
ice.org.uk

Registered charity number 210252.
Charity registered in Scotland number SC038629.

Printed on paper made from sustainable resources.

ice