Australian Government
Security Construction and Equipment Committee

SCEC-Endorsed Security Zone Consultant Scheme policy

Handling instructions

This document must be handled in accordance with its security classification and its protective markings, as prescribed by the Protective Security Policy Framework and the *Australian Government security caveat guidelines*.

Disclaimer

The Commonwealth, its officers, employees, and agents exclude all liability for loss or damage (including in negligence) suffered or incurred by any organisation or individual as a result of their use of or reliance upon the information contained in this document.

Inquiries

Inquiries should be addressed to:

Email: scec@scec.gov.au

Release history

Version No.	Release date	Amendment
1	01-OCT-2017	First version
2	08-JUN-2021	Formatting update, separate Code of Conduct and application forms
3	20-JUN-2025	Formatting update, reporting requirements and content review

Contents

1 Introduction

The SCEC Endorsed Security Zone Consultant Scheme supports Australian Government departments and agencies to engage suitably qualified and experienced security professionals who can provide physical security advice on the:

- design, acceptance testing[1] and commissioning[2] of Type 1A Security Alarm Systems (Type 1A SAS) in accordance with the requirements of the *Type 1A SAS Implementation and Operation Guide*; and
- design and construction of Security Zones as defined in the Australian Government *Protective Security Policy Framework* (PSPF) and ASIO *Technical Notes*.

The PSPF requires Australian Government departments and agencies **must** engage a SCEC Endorsed Security Zone Consultant (SCEC Consultant) for the design, acceptance testing or commissioning of a Type 1A security alarm system. The PSPF also states that Australian Government departments and agencies may choose to engage a SCEC Consultant to assist with the design and construction of security zones.

This document details the policy, procedures and eligibility requirements for the SCEC Endorsed Security Zone Consultant Scheme. This policy sets out the approval criteria and process to be used by SCEC in assessing applicants for the scheme, and sets out the rights and responsibilities of the applicants.

Approval is dependent on meeting the application criteria, and being assessed as a 'fit and proper' person (see section 8).

SCEC Security Zone Consultants are independent security professionals who have qualifications in the electrical or electronics engineering disciplines, and who have demonstrated relevant experience in the security industry. Applicants and SCEC Security Zone Consultants **must** note:

- endorsement is valid for five years;
- a minimum Negative Vetting Level 1 (NV1) security clearance is required—SCEC can sponsor a security clearance or be an 'interested party' to an existing security clearance;
- endorsement is subject to ongoing compliance with the requirements detailed in this policy; and
- applicants and SCEC consultants will incur all costs associated with their respective initial endorsement and re-endorsement – this includes the cost of obtaining and maintaining a minimum NV1 security clearance.

Applicants that meet the consultant scheme eligibility requirements will be provided with:

- a briefing outlining the responsibilities under the scheme and ongoing responsibility under and Parts 5.2 and 5.6 of the *Criminal Code 1995* (Cth) covering the protection of official information;
- a photographic SCEC Consultant identification card as evidence of their SCEC-endorsement; and
- login credentials to the SCEC website www.scec.gov.au to access the Security Equipment Evaluated Products List (SEEPL), Protective Security Circulars (PSCs) and Security Equipment Guides (SEGs).

A list of current SCEC Endorsed Consultants is available on the GovTeams Protective Security Policy community page www.govteams.gov.au (accessible with a.gov.au email address and at www.scec.gov.au.

[1] 'Acceptance testing' is performed to check if the requirements of a specification or contract are satisfied. Testing may involve electrical, physical, or performance tests.

[2] 'Commissioning' is the process of ensuring that all systems and sub-components of the project are designed, installed, tested, operated, and maintained according to the owner's operational requirements.

2 Objective

The objective of this policy is to detail:

- the criteria used by SCEC in assessing an applicant's suitability for endorsement and re-endorsement as a SCEC Consultant;
- the rights and responsibilities of applicants and SCEC Consultants; and
- the circumstances whereby SCEC may revoke (permanently terminate) or suspend (for a period determined by SCEC) a SCEC Consultant's endorsement.

SCEC reserves the right to:

- amend this policy at any time; amendments will be communicated to applicants and SCEC Consultants and, unless specified otherwise, must be complied with within six months from the date of notification—amendments will be published on the SCEC website;
- seek confirmation or clarification on the information submitted in applications, including contacting nominated referees or make independent inquiries;
- determine whether an application for endorsement or re-endorsement meets the requirements detailed in this policy; and
- determine if a Consultant has failed to meet the ongoing obligations and/or requirements of a SCEC Consultant.

3 Purpose of the SCEC Endorsed Security Zone Consultant Scheme

The purpose of the SCEC Endorsed Security Zone Consultant Scheme (Consultant Scheme) is to support Australian Government departments and agencies to engage suitably qualified and experienced security professionals who can assist with the design, acceptance testing and commissioning of Type 1A SAS and advise on the construction of security zones.

The PSPF states that the commissioning of a Type 1A SAS is only permitted to be undertaken by a SCEC Consultant. From the SCEC Consultant's perspective, commissioning is completed using a witness testing process where the installer of the Type 1A SAS demonstrates that the installation meets the design requirements with the results recorded in a Commissioning Certificate by the SCEC Consultant.

Entities seeking assistance with the design and construction of security zones may choose to engage a SCEC Consultant or a private sector security consultant.

When designing appropriate security zones and Type 1A SAS installations, entities rely on the knowledge and skills of the SCEC Consultant to protect their information, assets, and people. Over the course of the engagement, the SCEC Consultant is likely to gain a deep understanding of the security of the premises and security arrangement of the engaging entity. As such, it is important that the SCEC Consultant is trustworthy and capable; the SCEC applicant assessment and re-endorsement processes and the requirement for a current NV1 security clearance, are designed to provide this assurance for entities.

4 Application process

Security professionals seeking SCEC endorsement should monitor the SCEC website for advice on when a window is open for submitting applications. New applications will not be accepted outside the advertised periods.

An applicant's suitability will be determined using the information provided by the applicant against the eligibility requirements outlined at part 5.

Applicants will be advised of any concerns that SCEC may have with their application. If the concerns are not mitigated, then the SCEC Chair will advise the individual of the concerns in writing. The individual will be given reasonable time to answer the concerns in writing before a final decision is made on whether the application will progress.

At any stage during the application process, the SCEC Chair may:

- request further information or documentation to support an application;
- request additional referees or previous client contact details to assist in substantiating claims made in the application; or
- refuse an applicant on the basis of national security considerations. The reasons for concern may not be advised to an applicant if the disclosure is prejudicial to the interests of security.

Application forms are available on the SCEC website. Applicants must submit a completed application form and provide all requested supporting documentation as set out in this policy. Only complete applications will progress. Applications must be sent to:

Email: scec@scec.gov.au

To assist applicants, a checklist is provided as part of the application form to ensure all the required documentation is submitted and to minimise potential delays in processing an application. If you have any questions or require assistance please contact scec@scec.gov.au

5 Application assessment

Only applications from security professionals that meet the minimum requirements listed below will progress. Meeting these requirements does not imply an applicant will be accepted into the scheme, as SCEC assesses each applicant individually for suitability.

Applicants must be able to demonstrate one of the following qualification requirements:

Applicants must have a diploma (or higher) in electrical or electronic engineering (or equivalent deemed acceptable by SCEC or recognised professional / industry body) and a minimum of four years electronic security consulting experience within the past seven years from the date of their application.

OR

Applicants must have a Certificate IV (or equivalent) in electrical or electronic engineering (or equivalent deemed acceptable by SCEC) and a minimum of six years electronic security consulting experience within the past nine years from the date of application.

OR

Applicants with no formal electrical or electronic engineering qualifications may be considered if they can demonstrate a minimum of seven years consulting experience in electronic security within the last 10 years from the date of application.

SCEC defines commercial consulting experience as:

- *experience derived from employment in an ABN registered business that provides independent consulting exceeding seven years; and*
- *experience tendering, designing, construction and commissioning of electronic security products.*
- *SCEC does not recognise government employment in a security advisory capacity as a commercial consulting experience.*
- *Applicants must provide evidence to substantiate having designed and conducted formal commissioning or acceptance testing of at least five Electronic Access Control Systems (EACS) or Security Alarm Systems (SAS)within five years of the date of application, at least two of which were: for a government agency; and*
- *used commercial-grade equipment for commercial premises (not domestic/residential purposes).*

Applicants must provide evidence of having designed or been involved in the application of physical security measures Including commercial consulting experience.

The following referee reports must be submitted in support of an application:

- a supervisor referee report for at least one electronic security project involving the installation of an EACS or SAS;
- two client referee reports (must be different clients) from two separate security fit-outs for which the applicant has managed the design, construction and implementation of electronic and physical security measures.

The reports must include:

- *the scope of the project.*
- *the size and location of premises.*
- *the electronic and physical security systems used (type and manufacturer).*
- *the applicant's level of involvement (duties, dates and timeframe).*
- *the referee's opinion on the applicant's performance throughout the project; and*
- *the referee's opinion on the applicant's suitability to fulfil the obligations of the role.*

Where applicable, applicants must have the appropriate state and/or territory security licence to undertake security services in the state or territory of the primary place of business.

Applicants must:

- be an Australian citizen;
- be a fit and proper person of good reputation, integrity and character, including being honest and trustworthy. These characteristics are assessed through the provided referee reports; and
- be able to obtain and maintain a minimum-security vetting clearance of NV1. For further details on this requirement, applicants can refer to the Australian Government Security Vetting Agency Guidelines at https://www.agsva.gov.au http://www.defence.gov.au/agsva/Factsheets-Forms/.
- A national police check completed by the Australian Federal Police (state police checks are not acceptable). Under Section 8, 'Purpose of Check', please select 'Code 40 – Other Commonwealth Purpose ONLY', a fingerprint check is not required, and there are no exclusions under the spent convictions scheme; This AFP

records check must be dated within 12 months from the date the complete application pack to the scheme is submitted.

The scheme provides for periodic renewal of each consultant's approval status, this includes compliance with the SCEC-approved code of conduct policy and continued assessment as a fit and proper person.

All decisions to reject a consultant's application will be subject to the procedural fairness to the fullest extent possible, consistent with national security requirements. Applicants will be advised verbally of any concerns that SCEC may have regarding their application, or continuing participation in the scheme. If the concerns are not mitigated verbally, the Chair of SCEC will advise the applicant of the concerns in writing and the applicant will then be given reasonable time to address the concerns before a final decision is made.

6 Conditions of endorsement

Applicants accepted to the scheme must agree to the following conditions prior to being endorsed.
All SCEC Consultants must comply with the following conditions. Failure to comply or notify SCEC of changes in circumstances may adversely affect any application or lead to the suspension of endorsement pending an investigation.

Security clearance and vetting

Applicants are required to obtain a minimum NV1 security clearance to become SCEC endorsed Applicants unable to obtain or maintain a minimum NV1 cannot be part of the scheme. Australian citizenship is a prerequisite to obtaining an NV1.

SCEC is able to sponsor a new NV1 security clearance or be an 'interested party' to an existing NV1 security clearance. The costs incurred by SCEC associated with sponsoring an NV1 clearance must be reimbursed by the applicant to become SCEC endorsed.

Personnel accessing internal components of the Type 1A SAS (including any person having programming access to the Intruder Alarm Panel, Data Gathering Panel, Central Supervisory System or Type 1A sensor endpoint containing an end-of-line module) must hold a NV1 security clearance at minimum. However, clearances must be at least equal to the classification of the system accessed, therefore some entities may require higher level clearances in some circumstances. SCEC will not sponsor higher level clearances.

Any costs incurred by SCEC for sponsoring an applicant's security clearance must be reimbursed by the applicant regardless of the outcome.

Consultant briefing and induction

Applicants must attend the briefing provided by SCEC. Courses will be held regularly subject to a minimum number of applications being received.

Compliance agreement

Applicants must certify in writing that they will meet the requirements of this policy, including responsibilities under the Scheme and ongoing responsibility under Parts 5.2 and 5.6 of the Criminal Code (Cth) covering the protection of official information.

Code of conduct

SCEC Consultants must acknowledge in writing and comply with the code of conduct at all times (refer Annex A).

SCEC Consultants must at all times demonstrate a level of integrity and reliability sufficient to assure SCEC that the person can be entrusted with Australian Government resources. This includes demonstrating:

- Integrity: soundness of character and moral principle;
- Reliability: trustworthy, responsible and dependable; and
- Fit and proper person: defined in Australian Security Adjudicative Standard see PSPF 'Chapter 19.2'.

Conflict of interest

SCEC defines a conflict of interest as a situation in which a SCEC Consultant is in a position of trust but has competing professional or personal interests. Such competing interests can make it difficult for a SCEC Consultant to fulfil duties impartially, and could potentially influence the performance of their duties and responsibilities. Conflicts of interest may be real or apparent:

- Real: Where a direct conflict exists between current duties as a SCEC Consultant and existing private interest. For example, SCEC considers being both an employee of a Type 1A SAS supplier and a SCEC Consultant to be a conflict of interest.
- Apparent: Where it appears or could be perceived that private interests are improperly influencing the performance of duties, whether or not that is actually the case. For example, SCEC considers being both a government employee, or employee/owner of a SCEC-endorsed security product manufacturer/supplier, and being a SCEC Consultant to be a potential conflict of interest and would preclude a person from being accepted into the scheme.

SCEC takes any real or apparent conflicts of interest seriously and handles all declarations confidentially. Applicants deemed by SCEC to have a real or apparent conflict of interest in performing the role of a SCEC Consultant may be excluded from participating in the scheme.

Failure to declare a conflict of interest is deemed a breach of this policy and will result in the suspension and possible revocation of the SECEC Consultant's endorsement pending further investigation by SCEC.

SCEC-endorsed consultant identification card

The SCEC identification card is proof of a consultant's suitability and endorsement under the scheme and is to be provided to Australian Government agency personnel on request. The card:

- must be worn at all times when conducting work on an Australian Government agency premises;
- remains the property of the SCEC at all times—it is to be immediately returned to the SCEC Chair on request or when ceasing to perform the role of a SCEC Consultant; and
- returned if SCEC revokes endorsement or suspends endorsement for the period of suspension.

Provision of consultant services

SCEC Consultants are expected to remain current with changes in the industry and provide security best-practice solutions to Australian Government clients that meet the requirements of the scheme. If requested by the SCEC, SCEC Consultants must be able to produce evidence that they have provided advice to an Australian Government agency over the preceding two-year period on:

- the design, acceptance testing and commissioning of Type 1A SAS; or
- the design and construction of security zones defined in ASIO Technical Notes.

SCEC Consultant Refresher Briefings

SCEC will periodically schedule refresher briefings with SCEC Consultants. This will be an opportunity for SCEC to provide Consultants with updates on policy and specifications as well as a forum for open discussion on issues or concerns being encountered and corrective actions.

SCEC Consultants must satisfy SCEC requirements with regard to ongoing learning and development. This would include a requirement to attend SCEC refresher briefing days and/or keep up to date with SCEC advisories (such as the SCEC Consultant Bulletin) as part of ongoing endorsement.

Change of circumstances

SCEC Consultants must advise SCEC of any changes in circumstances that may affect their continued endorsement within 21 calendar days, including:

- no longer being employed as a SCEC Consultant;
- changes to their security licences—new (additional states or territories), rejected, suspended, revoked or expired;
- their security vetting clearance being denied or revoked;
- being the subject of an official investigation by a government entity or law enforcement agency;
- being charged with a criminal offence;
- being convicted of a criminal offence; and
- any changes in details as submitted in the application form, including but not limited to changes in employer, address or contact details.
- Being subject to an investigation or adverse findings of a professional / industry body

Maintaining your clearance

The initial security vetting process provides a snapshot of an individual at a particular point in time. Once you have been granted a security clearance there are a number of responsibilities and actions that need to be met to ensure your ongoing suitability to hold a security clearance. Your ongoing responsibilities to maintain your clearance will be advised to you when clearance is granted, amongst other requirements this will include reporting changes in your personal circumstances or any suspicious or unusual approaches made to you relating to your professional duties. For more information please refer to the PSPF policy 13: Ongoing assessment of personnel.

Changes to your personal situation including change of name or identity, change in citizenship or nationality, relationships, finances and associations may affect your security clearance and need to be notified to the Australian Government Security Vetting Agency (AGSVA) as well as SCEC. This is done via the myClearance portal on AGSVA's website: agsva.gov.au/clearance-holders/reporting-changes as is a comprehensive list of changes that must be reported. A change of circumstances form is available on the SCEC website which will also need to be completed.

When SCEC is satisfied all the required conditions have been met, a photographic SCEC Consultant identification card will be issued to the SCEC Consultant as evidence they have successfully completed the process and are SCEC endorsed. The SCEC Consultant's details will be added to the SCEC Consultant listing and published on the SCEC website.

SCEC Consultants will be issued with login access to the SCEC website www.scec.gov.au to use the SEEPL to select SCEC-approved security equipment and access relevant ASIO Technical Notes and publications. SCEC consultants must periodically access the SCEC website via their logon to monitor for changes to policy, updated documentation or other SCEC notifications which are relevant to the scheme.

7 Applications for re-endorsement

The approval status of SCEC-endorsed consultants will expire after five years. Consultants wishing to remain in the scheme must submit a completed SCEC-Endorsed Security Zone Consultant Scheme - application for re-endorsement found at www.scec.gov.au.

SCEC Consultants applying for renewal must comply with the directives listed via their login access to the SCEC website and submit a re-endorsement application form no later than six months before the endorsement expiry date.

SCEC will consider and assess a SCEC Consultant's ongoing suitability to remain in the scheme against the information provided and the assessment criteria (refer part 10). The assessment will take into consideration all information provided as part of the re-endorsement process as well as previous applications.
A SCEC Consultant's endorsement may be reassessed at any time if:

- policy or technological changes warrant additional training requirements;
- feedback received from government clients calls into question the validity of advice provided;
- a competency assessment is warranted; or
- concerns about the continuing suitability, or ability to maintain a security clearance, are reported to, or identified by, SCEC.

A SCEC consultant cannot reapply if their endorsement has been revoked. A SCEC consultant can reapply to be considered for the scheme as a new applicant if:

- their endorsement is allowed to expire and there has been no re-endorsement application submitted or correspondence provided by SCEC advising otherwise;
- a SCEC consultant notifies SCEC and leaves the scheme due to personal reasons or change of employment and more than 6 months has expired; or
- re-endorsement requirements as set out in the assessment criteria (refer section 10) of this policy are not met.

SCEC Consultants seeking to renew their endorsement must comply with the requirements of this policy. Failure to comply with the policy or notify SCEC of changes in circumstances may adversely affect any application or lead to the suspension of endorsement pending an investigation. SCEC will discontinue sponsorship of a consultant's security clearance when they are no longer part of the scheme.

Compliance agreement

SCEC Consultants are reminded of their agreement to ensure the requirements of this policy are met on an ongoing basis, including responsibilities under the scheme and ongoing responsibility under Part 5.2 and 5.6 of the Criminal Code 1995 (Cth) covering the protection of official information.

Consultant code of conduct

SCEC Consultants must acknowledge in writing and comply with the consultant code of conduct at all times (refer Annex A).

Conflict of interest

SCEC Consultants applying for re-endorsement must submit a completed and signed conflict of interest declaration form, available on the SCEC website, as part of the application. When a consultant becomes aware of a conflict they must immediately report it in writing to their employing government agency and SCEC, including pecuniary (financial) interests and non-pecuniary (personal) interests. For more information about conflicts of interest refer to Part 6.

Provision of consultant services

SCEC Consultants are expected to remain current with changes in the industry and provide security best-practice solutions for clients that meet the requirements of the scheme. SCEC Consultants must be able to produce evidence that they have provided advice to an Australian government agency during the endorsement period on:

- the design, acceptance testing and commissioning of Type 1A SAS; or
- the design and construction of security zones defined in ASIO Technical Notes.

SCEC Consultants maybe required to provide one referee report for both of the above areas of advice from the client (agency security adviser or Australian government agency project manager).

SCEC Consultant refresher briefings

SCEC Consultants must satisfy SCEC requirements with regard to ongoing learning and development. This would include a requirement to attend SCEC refresher briefing days and/or keep up to date with ASIO advisories (such as the SCEC Consultant Bulletin) as part of ongoing endorsement.

SCEC briefing days will be held on a as required basis. The briefing days provide updates to policy and specification relevant to SCEC Consultants fulfilling the role as well as a forum for open discussion on issues or concerns being encountered.

Security vetting clearance

SCEC Consultants are required to hold a minimum NV1 security clearance.

SCEC Consultants unable to maintain the minimum clearance cannot be part of the scheme.

Personnel accessing internal components of the Type 1A SAS (including any person having programming access to the Intruder Alarm Panel, Data Gathering Panel, Central Supervisory System or Type 1A sensor endpoint containing an end of line module) must hold a NV1 security clearance at minimum. However, clearances must be at least equal to the classification of the system accessed, therefore higher-level clearances may be required in some circumstances, noting SCEC will not sponsor these higher-level clearances.

8 Fit and proper person assessment

Applicants will be assessed against the following criteria based on documentary evidence provided by the applicant and other checks as detailed below.

Applicants must continue to be considered fit and proper persons. Failure to continue to meet the high standards expected of SCEC-approved consultants will lead to suspension and/or revocation of the SCEC approval.

Personal qualities

The applicant is to be of good reputation, integrity, and character, including being honest, trustworthy, and mature. These characteristics are to be confirmed by referee report and results of the AFP Records check. The Personal Security Adjudicative Guidelines, available from protectivesecurity.gov.au, are to be used as a guide when assessing the applicant's suitability against the "Whole Person". Any mitigating factors as identified in the Adjudicative Guidelines should be considered prior to making an adverse determination against the applicant

Criminal offences

The applicant must not have been convicted of any offences:

1) Involving fraud, theft, or dishonesty; and/or,
2) Related to national security such as threat of terrorism, politically motivated violence, or threats against holders of high office.

Offences are to be declared in accordance with the *Spent Convictions Scheme of the Crimes Act 1914 (Cth)*. SCEC is not subject to any exclusions under the scheme.

A history of multiple or recent offences other than the types listed above may lead to a decision of the applicant being unsuitable.

If granted approval to the scheme the applicant is to advise SCEC of any criminal charges laid against the applicant during the course of their participation in the scheme. Failure to advise of changes may result in revocation of approval.

ASIO assessment

All applicants may undergo an ASIO holdings check conducted on behalf of the SCEC. Where areas of concern are identified, an ASIO security assessment may be initiated. Any unresolved concerns from the ASIO security assessment may disqualify the applicant from the scheme.

9 Changes of circumstances

SCEC-approved consultants must advise SCEC, via the SCEC-Endorsed Security Zone Consultant Scheme - change of circumstance form found at www.scec.gov.au, of any changes in circumstances that may affect their continued approval within 14 calendar days, including:

1) No longer being employed as a consultant;
2) Changes to security licences—new (additional states or territories), rejected, suspended, revoked or expired;
3) Being the subject of an official investigation by a government entity or law enforcement agency;
4) Being charged with a criminal offence;
5) Being convicted of a criminal offence; and,
6) Any changes in details as submitted in the application form, including but not limited to changes in employer, address, or contact details.
7) Being subject to an investigation or adverse findings of a professional / industry body

Failure to report changes in circumstances may result in revocation of SCEC approval.

10 Conditions of approval

SCEC-approved Security Zone Consultant briefing

Applicants must attend a briefing by ASIO on behalf of SCEC. The briefing will include information relevant to the duties of a SCEC-approved consultant, and will include a statement of ongoing responsibility under sections 70 and 79 of the *Crimes Act 1914 (Cth)* and part 5.2 of the *Criminal Code Act 1995 (Cth)* covering for the protection of official information.

SCEC-approved consultants Code of Conduct

All participating consultants must comply with the *SCEC Endorsed Security Zone Consultant Scheme - Code of Conduct* while participating in the scheme. All reported instances of non-compliance will be investigated by SCEC, and if found to be true may lead to suspension and/or revocation of approval under the scheme.

SCEC-approved Security Zone Consultant identification card

All participating consultants will be provided with a photographic SCEC-approved Security Zone Consultant identification card. This card must be provided to Australian Government agency security personnel on request.

This identification card must be worn at all times when undertaking work as a SCEC-approved Security Zone Consultant for Australian Government agencies.

Lost or stolen SCEC-approved Security Zone Consultant identification card

Where a SCEC-approved Security Zone Consultant identification card has been lost, cannot be located, or has been stolen, the consultant must complete the *SCEC-Endorsed Security Zone Consultant Scheme - lost and stolen identification card* form found at www.scec.gov.au, and submit to SCEC as soon as practicable.

Once the lost and stolen identification card form has been received by SCEC, a new identification card may, at the discretion of SCEC, be issued to the participating consultant.

11 Revocation of approval

SCEC will suspend participants from the scheme when it becomes aware of credible information that is relevant to whether a SCEC-approved Security Zone Consultant is a fit and proper person. If, following an investigation, the concerns are found to be true and are not otherwise mitigated, the consultant's approval may be revoked. Grounds for revocation include:

1) Providing false or misleading information to any Australian Government agency, official, or representative, including during the SCEC-endorsed Security Zone Consultant Scheme application process;
2) Breaching any of the Conditions of Approval (See section 10);
3) Being convicted of an offence;
4) No longer being employed as a consultant;
5) Not having, or no longer having, the necessary State and/or Territory security licenses; and,
6) Where technological advancements warrant additional training or competency assessment. However, under this circumstance, SCEC will set a grace period for each consultant to address the new training requirements and, if required, sit a competency assessment before revocation is considered.

All decisions to reject a consultant's application will be subject to the procedural fairness to the fullest extent possible, consistent with national security requirements. Applicants will be advised verbally of any concerns that SCEC may have regarding their application, or continuing participation in the scheme. If the concerns are not mitigated verbally, the Chair of SCEC will advise the applicant of the concerns in writing and the applicant will then be given reasonable time to address the concerns before a final decision is made.

Participants who have their approval revoked must return their SCEC-approved Security Zone Consultant identification card. SCEC will remove their details from the SCEC-approved consultants list, and advise Australian Government agencies of the revocation.

Notification of application decision

The SCEC will notify the outcome of all applications in writing within 28 days of the decision.

Acceptance

SCEC will notify all applicants who are selected to participate in the SCEC-approved Security Zone Consultant Scheme in writing. The notification will include:

1) The letter of acceptance into the scheme;
2) Joining instructions for the SCEC-endorsed Security Zone Consultant briefing

Rejection or revocation

SCEC will discuss any issues with applicants to the scheme prior to providing formal notification of rejection, unless they are unable to be disclosed for national security reasons. This will provide the applicant with an opportunity to address the identified issues.

The Chair of the SCEC will provide all applicants who are found to be unsuitable for participation in the scheme with written advice stating the grounds for unsuitability, unless the information cannot be provided for national security reasons.

The written advice from the Chair of SCEC will include:

1) Advice on procedural fairness; and,
2) Details of the review process.

Participants who have their approval revoked must:

3) Return their SCEC-endorsed Security Zone Consultant identification card; and,
4) Remove all references to participation in the SCEC Security Zone Consultant Scheme from all marketing and promotional material.

SCEC will also:

5) Remove the participant from the SCEC-approved consultants list; and,
6) Advise Australian Government agencies of the revocation.

12 Appeal process

To appeal an application rejection or a participant's revocation, the consultant must submit the appeal request in writing to the Chair of SCEC, within 28 days of the decision date, and include all details the consultant deems relevant to the appeal.

The Chair of the Government Security Committee (GSC), as the committee overseeing the SCEC, may undertake a review of SCEC's decision.

The GSC will review the application, assessment process, and reasons for rejection or revocation, as well as any additional information provided in writing by the applicant. The reviewing officer may then:

1) Uphold the SCEC decision; or,
2) Overturn the SCEC decision.

The applicant will be notified in writing no more than 28 days after the conclusion of the appeal decision.

13 Provision of services

SCEC-approved consultants are expected to remain current with changes in the industry, and provide security best-practice solutions, and the highest standard of work, to Australian Government clients.

SCEC-approved consultants are also expected to remain familiar with all other policy and guidance documents relating to SCEC-approved devices and systems, and working within Australian Government security zoned facilities. These documents include, but are not limited to:

a) ASIO Technical Note 1/15 Physical Security Zones;
b) ASIO Technical Note 5/12 Zone 5 (Top Secret) areas;
c) ASIO Technical Note 7/06 Class A Secure Rooms;

d) ASIO Technical Note 8/06 Class B Secure Rooms;
e) ASIO Technical Note 9/06 Class C Secure Rooms;
f) Protective Security Policy Framework 15 Physical security for entity resources;
g) Protective Security Policy Framework 16 Entity facilities;
h) Security Equipment Evaluated Product List (SEEPL);
i) All relevant Security Equipment Guides; and,
j) ASIO bulletins

All current policy and guidance documents of relevance to SCEC-endorsed consultants can be found at www.scec.gov.au and will be accessible once the consultant has received SCEC-endorsed Security Zone Consultant login access to the website.

14 Consultant assessment criteria

Consultant assessment criteria			
Qualifications—applicants will be assessed against one of the following criteria depending on existing qualifications			
Applicant holds a Diploma (or higher) in Electrical or Electronic Engineering		New application	Re-endorsement
1.1	Must have a Diploma (or higher) in Electrical or Electronic Engineering (or equivalent deemed acceptable by SCEC) and a minimum of four years electronic security consulting experience within the past seven years that is current.	✔	-
1.2	Must have conducted formal commissioning or acceptance testing of at least five electronic security systems within the past five years, comprising Electronic Access Control Systems (EACS) or Security Alarm Systems (SAS), at least two of which were: • for a government agency; and • an SAS with commercial-grade equipment (not domestic/residential premises).	✔	-
1.3	Must provide a supervisor referee report for one electronic security project (EACS or SAS).	✔	-
1.4	Must provide two referee reports from two separate security fit-outs (design and construction of physical security measures) which the consultant has managed.	✔	-
1.5	Applicants must have the requisite/necessary state and/or territory security licence to undertake SCEC services.[3]	✔	✔
Applicant holds a Certificate IV (or equivalent) in Electrical or Electronic Engineering			

[3] Unless the identified State or Territory does not issue licenses to security consultants and/or security alarm installers.

2.1	Must have a Certificate IV (or equivalent) in Electrical or Electronic Engineering (or equivalent deemed acceptable by SCEC) and a minimum of six years electronic security consulting experience within the past nine years that is current.	✔	-
2.2	Must have conducted formal commissioning or acceptance testing of at least five electronic security systems within the past five years comprising EACS or SAS, at least two of which were: • for a government agency; and • an SAS with commercial-grade equipment (not domestic/residential premises).	✔	-
2.3	Must provide a supervisor referee report for one electronic security project (EACS or SAS).	✔	-
2.4	Must provide two referee reports from two separate security fit-outs (design and construction of physical security measures) which the consultant has managed.	✔	-
2.5	Applicants must have the requisite/necessary state and/or territory security licence to undertake SCEC services.	✔	✔
Applicant holds no formal electrical or electronic engineering qualifications (regardless of other qualification)			
3.1	Applicants with no formal Electrical or Electronic Engineering qualifications may be considered if they can demonstrate within the last 10 years a minimum of seven years consulting experience in electronic security that is current.	✔	-
3.2	Must have conducted formal commissioning or acceptance testing of at least five electronic security systems within the past five years comprising EACS or SAS, at least two of which were: • for a government agency; and • an SAS with commercial-grade equipment (not domestic/residential premises).	✔	-
3.3	Must provide a supervisor referee report for one electronic security project (EACS or SAS).	✔	-
3.4	Must provide two referee reports from two separate security fit-outs (design and construction of physical security measures) which the consultant has managed.	✔	-
3.5	Applicants must have the requisite/necessary state and/or territory security licence to undertake SCEC services.	✔	✔
General criteria—all applicants are assessed against the following criteria			
Personal			
4.1	Must be an Australian citizen.	✔	✔

4.2	Must meet the requirements and be willing to submit to a minimum-security vetting clearance of NV1.	✔	-
4.3	A national police check completed by the Australian Federal Police	✔	✔
4.4	Must demonstrate a level of integrity and reliability sufficient for the SCEC Committee to be assured the person can be entrusted with its Australian Government resources: • Integrity: soundness of character and moral principle. • Reliability: trustworthy, responsible and dependable.	✔	✔
4.5	Must comply with the consultant code of conduct at all times.	✔	✔
4.6	Must agree to assessment against ASIO information holdings.	✔	✔
4.7	Must report change of circumstance in accordance with policy requirements.	✔	✔
4.8	Must sign an initial declaration and report conflict of interest in accordance with policy requirements.	✔	✔
4.9	Must maintain and comply with the requirements of this policy on an ongoing basis, including responsibilities under the scheme and ongoing responsibility under Parts 5.2 and 5.6 of the Criminal Code (Cth) covering the protection of official information.	✔	✔
Re-endorsement			
5.1	Must satisfy SCEC requirements with regard to ongoing leaning and development. This would include a requirement to attend SCEC briefing days and/or keep to date with SCEC advisories (such as the SCEC Consultant Bulletin) as part of ongoing endorsement.	-	✔
5.2	Must provide evidence of having conducted: • design, acceptance testing and commissioning of Type 1A SAS; and • design and construction of Australian Government security zones as defined in the PSPF and ASIO Technical Notes At least twice since the date of endorsement (or previous re-endorsement) or previous re-endorsement. This should be in the form of referee reports; a template is included in the renewal applications form. Referee reports must be from at least two separate client agencies.	-	✔
5.3	Must hold a minimum NV1 security clearance.	-	✔

Annex 1 SCEC-Endorsed Security Zone Consultant Scheme Code of conduct

When acting in the course their work for the Australian Government, Australian Public Service (APS), or any other SCEC related work, a SCEC-endorsed consultant must:

1) Behave honestly and with integrity;
2) Act with care, diligence, and best practice;
3) Treat all persons with respect and courtesy, and without harassment;
4) Comply with all Australian laws;
5) Maintain confidentiality about any dealings or work conducted as a SCEC-endorsed consultant;
6) Take reasonable steps to avoid any conflict of interest (real or apparent), and where this is not possible, disclose any conflict of interest (real or apparent) in writing to SCEC as soon as possible;
7) Use Commonwealth resources in a proper manner;
8) Not provide false or misleading information;
9) At all times behave in a way that upholds the integrity and good reputation of SCEC; and,
10) Not make improper use of:
    a. Privileged information;
    b. The consultant's duties, status, power or authority.
11) Complete work to the highest professional standard
12) Report all changes of circumstances to SCEC as referred to in the SCEC endorsed Security Zone Consultant Scheme Policy.