CPNI
Centre for the Protection of National Infrastructure

END OF LIFE OF A BUILT ASSET, INCLUDING A CHANGE IN ASSET OWNER/OCCUPIER

MANAGING THE SCA PROCESS

A SCA should be undertaken at the end of life of a built asset, including a change of owner or occupier, where failure to take appropriate measures could result in precise details about security risks and mitigation methods being revealed. The asset owner(s) should therefore ensure that processes are in place, and implemented, to initiate the SCA process at the start of the project.

These processes should include the nomination of a suitable individual who will be responsible for initiating and managing the associated SCA process. The individual fulfilling this role should be employed by, or report directly to, the asset owner's organisation.

The individual responsible for initiating and managing the SCA process on behalf of the commissioning organisation should ensure that an appropriately qualified and experienced specialist or small team of two or more specialists is appointed to undertake a SCA (see 'Undertaking a Security Considerations Assessment').

It is important that sufficient notice of when a SCA will be required is given, with each of the relevant parties agreeing a timeframe for completion.

THE SCA STAGES

A Stage 1 SCA facilitates embedding of security-mindedness from the planning stages of the project when access to project information and potential sensitivities is limited to a relatively small group of individuals.

A Stage 2 SCA provides an opportunity for any security issues to be reviewed and, where necessary, re-elevated before the project moves from planning to delivery.

A Stage 3 SCA is only required if the built asset is being transferred to a new owner or occupier, rather than being demolished. In the case of the former, the SCA provides an opportunity to identify and address any outstanding security risks prior to handover of the asset.

There is no Stage 4 SCA for this type of activity.

Additional SCAs can be included as part of the procurement process for specialist contractors dealing with the removal of sensitive assets.

An interim SCA can be undertaken if there is concern or awareness that the nature of the threats or vulnerabilities has altered since the last SCA was undertaken. Under these circumstances, the list of documentation that would be provided for the next SCA stage due should be provided.

STAGE 1 SCA

Timing

Ideally, a Stage 1 SCA should be concluded in the initial planning of the end of life of the built asset, or its change of owner or occupier. At this time, specialist security advisers providing guidance in respect of relevant security threats, vulnerabilities and/or mitigations may also have been onboarded.

Scope

The Stage 1 SCA should:

1. list the information provided and record the information that is not available, noting the reason for this where provided;

2. review the security risk assessment documentation to identify any potential weaknesses in the process, in particular:

    a. any threats, vulnerabilities or risks which it would be appropriate and proportionate to include; and

    b. whether the documentation provides a robust record of the risk assessment process and outcome;

3. consider how security risk mitigation measures are reflected in policies, processes and planning of the new built asset;

4. identify and detail any gaps and inconsistencies within, and between, the documentation, policies and processes provided;

5. assess how policies and processes are being conveyed to those who need to follow them; and

6. for points 2 to 5 above, provide a summary of all the issues identified and set out appropriate and proportionate recommendations for addressing each issue.

Documentation required

The portfolio of information provided should include:

1. a summary of the built asset's current use, including layout, occupation, utilisation and accessibility to members of the public;

2. a summary of the project being undertaken;

3. details of any protection measures already in place;

4. documentation relating to:

    a. the identification of any sensitive assets that will need to be removed and/or asset information that will need to be protected;

    b. security risk assessment and mitigation; and

    c. identification of information already in the public domain;

5. where digital engineering techniques are going to be used in the public space's end of life, information security risk assessment and mitigation documentation;

6. the security-related policies and processes for the implementation of the selected mitigation measures;

7. the policies and processes in place for identifying, and responding to, security breaches and incidents, including near misses; and

8. the policies and processes in place for monitoring, auditing, reviewing and updating security risk management processes.

STAGE 2 AND 3 SCA

Timing

The Stage 2 SCA should be undertaken before decommissioning or demolition work begins.

A Stage 3 SCA is only required if the built asset is being transferred to a new owner or occupier, rather than being demolished, and should be conducted prior to the handover of the built asset.

Scope

The Stage 2 and 3 SCA should:

1. re-examine the previously identified and assessed risks to determine whether there have been any changes, whether for political, economic, social, technological, legal or environmental reasons;

2. review the effectiveness of the security measures implemented to date with an examination of any security breaches or incidents, including near misses;

3. examine the consistency of implementation of security mitigation measures;

4. review security-related monitoring and auditing activities undertaken;

5. review the issues raised in the previous report and reiterate any that have not been satisfactorily resolved and are still believed to be of importance.

Documentation required

The portfolio of information provided for each SCA stage should include, in addition to the documentation provided in the previous SCA:

1. the previous SCA and SCA response reports;

2. a summary of any changes to the project undertaken since the previous SCA;

3. details of any changes to:

   a. those aspects of the built asset considered to be sensitive;

   b. risk assessment and mitigation documentation;

   c. policies and processes for the implementation of security-related risk mitigation measures; and

   d. policies and processes for responding to security breaches and incidents;

4. details of any occurrences of security incidents and/or breaches and the actions taken at the time of, and subsequent to, the breach or incident; and

5. copies of reports from security-related monitoring and auditing undertaken.

ADDITIONAL SCAS – PROCUREMENT OF CONSULTANTS AND/OR CONTRACTORS

Timing

The first stage of this additional SCA should be undertaken prior to the issue of any tender for specialists consultants or contractors to support the project in question. The second stage should form part of the selection and final appointment process.

Scope

Prior to the issue of tender documentation, the additional SCA should review the security requirements set out in the tender documentation against the agreed security risk mitigation measures.

During the selection and appointment process, the additional SCA should:

1. assess the completeness of the submission documentation that relates to the security requirements;

2. identify and detail any issues that have not been addressed or appear to have been addressed insufficiently;

3. assess the consultant's or contractor's ability to deliver the relevant security mitigation measures and the extent of any support needed to enable them to fulfil the security requirements; and

4. provide a high-level assessment of the consultant's or contractor's organisational readiness to implement the required security measures.

Documentation required

The portfolio of information provided should include:

1. the tender documentation; and

2. the parts of the submission documentation that relate to the security requirements set out in the tender information.

Disclaimer

This guide has been prepared by CPNI and is intended to assist in undertaking a Security Considerations Assessment. This document is provided on an information basis only, and whilst CPNI has used all reasonable care in producing it, CPNI provides no warranty as to its accuracy or completeness.

To the fullest extent permitted by law, CPNI accepts no liability whatsoever for any expense, liability, loss, damage, claim or proceedings incurred or arising as a result of any error or omission in the report or arising from any person acting, refraining from acting, relying upon or otherwise using the document. You should make your own judgment with regard to the use of this document and seek independent professional advice on your particular circumstances.

CPNI
Centre for the Protection
of National Infrastructure