CPNI
Centre for the Protection of National Infrastructure

Plain Language Questions

August 2015

Plain Language Questions

Plain Language Questions (PLQs) are those questions that a client intends to answer at each stage of a construction project. The answers will enable key decisions to be made such as whether to proceed to the next work stage. It is recommended that the PLQs provided here are included with those relating to other aspects of a project where a client wishes a security-minded approach to be taken.

Stage 00 - Strategy

0/1 Is the built asset sensitive, in whole or in part?

Have considered whether the built asset may be of interest to a threat agent for hostile, malicious, fraudulent and/or criminal behaviours or activities.

0/2 Are any neighbouring built assets sensitive?

Have consulted with the owner/occupier/operator of any neighbouring built asset(s) to establish whether any measures need to be applied to information which will be shared, but which is not publicly available.

0/3 Is there a need for a security-minded approach?

Have undertaken the Security Triage process and determined whether a security-minded approach is required or, where business benefits may be derived, desirable.

0/4 Is a Built Asset Security Manager in place?

A suitably qualified and experienced individual has been appointed to fulfil the role of Built Asset Security Manager.

0/5 Is an approved Built Asset Risk Management Strategy is place?

*A Built Asset Risk Management Strat*egy *comprising risk assessment, risk mitigation and review processes is in place and it conforms with the requirements of PAS 1192-5:2015.*

0/6 Is an approved Built Asset Security Strategy (BASS) in place?

A *BASS which conforms with the requirements of PAS 1192-5:2015 is in place.*

0/7 Is an approved Built Asset Security Management Plan (BASMP) in place?

A *BASMP which conforms with the requirements of PAS 1192-5:2015 is in place.*

0/8 Is an approved Security Breach/Incident Management Plan (SB/IMP) in place?

SB/IMP which conforms with the requirements of PAS 1192-5:2015 is in place.

0/9 Is an approved Built Asset Security Information Requirements (BASIR) in place?

A BASIR which conforms with the requirements of PAS 1192-5:2015 is in place.

0/10 Are security-minded measures in place in relation to access given to information outside formal contracts, for example, in pre-contract dealings?

There is separation and suitable protection of sensitive information and data.

0/11 How will the security requirements as defined by the Built Asset Security Management Plan (BASMP) and Built Asset Security Information Requirements (BASIR) be met post-contract award?

Evidence of how the security requirements defined in the Employer's Information Requirements (EIR) will be met is included in submitted tender documentation.

Stage 01 - Brief

1/1 What data and/or information needs to be excluded from exchanges with third parties (e.g. planning authorities and other statutory authorities)?

There is separation and suitable protection of sensitive information and data.

Appropriate measures are in place for redaction of information and use of other protective measures.

Special handling arrangements have been discussed and agreed with the planning authority.

1/2 Are there measures in place for the handling, processing and storage of existing built asset information and survey data, including data or information relating to neighbouring built assets?

Appropriate and proportionate measures are in place to protect the data and/or information, and where appropriate, are consistent with the requirements of the neighbouring asset's owner/occupier/operator.

1/3 Are there suitable measures in place for the protection of personal and commercial data and/or information?

Confidentiality and non-disclosure agreements are contained in contractual documentation and access to and/or use of sensitive data is on a need-to-know basis.

1/4 Are there suitable measures in place for the protection of stakeholder data and/or information, for example property ownership along the route of an infrastructure project, environmental information etc.

Access to and/or use of data is on a need-to-know basis.

1/5 Is there appropriate management of information detailing: the security protection level or classification level of a project; security risk; and potential mitigation measures?

Information is handled on a strict need-to-know basis with security measures implemented in accordance with agreed risk management strategy.

1/6 Have high risk positions been identified within the project team and appropriate measures taken with regard to these positions?

High risk positions are identified, appropriate screening and vetting is in place and appropriate security-minded training is provided where necessary.

1/7 Has the use and nature of purpose-specific and/or volume-specific Construction Operations Building Information Exchange (COBie) files been agreed?

W*here appropriate, information pertaining to sensitive assets and systems will be contained in separate files.*

Stage 02 - Concept Design

2/1 Is there appropriate management of information detailing: the security protection level or classification level of a project; security risk; and potential mitigation measures?

Information is handled on a strict need-to-know basis with security measures implemented in accordance with agreed risk management strategy.

2/2 Do the models and accompanying data and information meet the requirements of the BASIR?

Models, data and information are consistent with the requirements of the BASIR.

2/3 Can the designers show that the project can be delivered in a security-minded way?

It can be shown that the delivery of the project can meet the requirements of the BASS and BASMP.

2/4 Have the BASS, BASMP and/or BASIR been reviewed in light of the additional information generated during the Concept stage?

Documents have been reviewed and updated, including review of changes in risk environment or changes in operational requirements.

Stage 03 - Definition/Developed Design

3/1 Is there appropriate management of information detailing: naming, category and functionality of areas, zones and assets; built asset usage (in whole or in part); and sensitive performance criteria?

Information is handled on a strict need-to-know basis with security measures implemented in accordance with agreed risk management strategy and at the level of detail consistent with the BASIR.

3/2 Where appropriate, have specialist sub-contractors have been utilised to provide information and guidance pertaining to the requirements and logistics of sensitive assets and systems?

Appropriate information is available to relevant members of the design team to assure correct specification of supporting infrastructure and planning for deployment of sensitive assets and systems.

3/3 Do the models and accompanying data and information meet the requirements of the BASIR?

Models, data and information are consistent with the requirements of the BASIR.

3/4 Have the BASS, BASMP and/or BASIR been reviewed in light of the additional information generated during the Definition stage?

Documents have been reviewed and updated, including review of changes in risk environment or changes in operational requirements.

Stage 04 - Design/Technical Design

4/1 Is there appropriate management of information detailing sensitive asset and system selection (including name, manufacturer, model number, performance and description) and connectivity?

Information is handled on a strict need-to-know basis with security measures implemented in accordance with agreed risk management strategy and at a level of detail consistent with the BASIR.

4/2 Is there appropriate management of data and information prepared by specialist sub-contractors in relation to sensitive assets and systems?

Information is handled on a strict need-to-know basis with security measures implemented in accordance with agreed risk management strategy and at a level of detail consistent with the BASIR.

4/3 (For most sensitive assets) Is the appropriate protection of information relating to the handling of emergency situations including evacuation procedures and contingency measures in place?

Information is handled on a strict need-to-know basis outside the employer's organisation and embedded third parties.

4/4 (For most sensitive assets) Is the appropriate protection of information relating to maintenance and facilities management of the asset in place?

Information is handled on a strict need-to-know basis outside the employer's organisation and embedded third parties.

4/5 Do the models and accompanying data and information meet the requirements of the BASIR?

Models, data and information are consistent with the requirements of the BASIR.

4/6 Have the BASS, BASMP and/or BASIR been reviewed in light of the additional information generated during the Design stage?

Documents have been reviewed and updated, including review of changes in risk environment or changes in operational requirements.

Stage 05 - Build/Construction

5/1 How will the construction site be managed securely?

Arrangements at the construction site are in accordance with the policies, processes and procedures set out in the BASMP and include measures to limit, or disrupt the success of, physical hostile reconnaissance.

5/2 Do the models and accompanying data and information meet the requirements of the BASIR?

Models, data and information are consistent with the requirements of the BASIR.

5/3 Have the BASS, BASMP and/or BASIR been reviewed in light of the additional information generated during the Build stage?

Documents have been reviewed and updated, including review of changes in risk environment or changes in operational requirements.

5/4 Is the installation of sensitive assets and systems scheduled so as to prevent unauthorised access and limit the potential for damage or compromise?

Installation of sensitive assets, and the fitting-out of sensitive areas is programmed for a time where access to those assets or areas can be limited to a number of specialist contractors, and where, for logistical reasons, this is not possible, appropriate and proportionate security measures are in place.

Stage 06 - Handover & Close Out

6/1 Do the models and accompanying data and information meet the requirements of the BASIR?

Models, data and information including information provided for operation and maintenance are consistent with the requirements of the BASIR.

6/2 Are measures being applied for the secure return, storage or destruction of asset information?

Procedures for post-contract management of information have been implemented.

6/3 Does the transfer of asset information to the Asset Information Model and the arrangements for access meet the requirements of the BASIR?

Models, data and information are consistent with the requirements of the BASIR. Access arrangements are in accordance with the BASMP.

6/4 Have the BASS, BASMP and/or BASIR been reviewed in light of the additional information generated during the Handover stage?

Documents have been reviewed and updated, including review of changes in risk environment or changes in operational requirements.

Stage 07 - Operation and End of Life

7/1 What security measures are required in the event that the built asset is significantly modified or decommissioned, or there is a change of ownership, occupancy or use?

Appropriate measures are in place to protect valuable, attractive and sensitive items, including all physical or information assets.