Infrastructure Protection Act - Guide for Responsible Person

As at December 2018

Every care has been taken to ensure the accuracy of the information contained in this guide at the time of publication. Please refer to the Infrastructure Protection Act and the related Subsidiary Legislations for the most up-to-date information on the Act.

Contents

INTRODUCTION 2
Objectives of this Document 2
Structure of this Document 2
CHAPTER 1 / Security By Design Framework and the IPA 3
What is Security By Design? 3
Who oversees the SBD process? 3
How does the SBD process work? 3
What buildings are required to undergo the SBD process under the IPA? 4
CHAPTER 2 / Management of Critical Infrastructure (CI) under IPA 5
Responsibility for security of CI under the IPA 5
Identification of CI 6
Designation of CI as Special Development / Special Infrastructure 6
Requirement to submit Security Plan for approval 6
Requirement to implement and maintain measures in Security Plan 8
Notification of change in RP of CI 9
Cessation of CI as Special Development and Special Infrastructure 9
CHAPTER 3 / Management of Large/Iconic Infrastructure under the IPA 10
Responsibility for security of large/iconic infrastructure under the IPA 10
Identification of large/iconic infrastructure 10
Designation of large/iconic infrastructure as Special Development / Special Infrastructure 11
Requirement to submit Security Plan for Approval 12
Requirement to implement and maintain measures in Security Plan 13
Notification of change of RP of large/iconic infrastructure 14
Cessation of large/iconic infrastructure as Special Developments and Special Infrastructure 14
CHAPTER 4: SBD Technical Guide 15
SBD Overview and Timeline 15
Application for Commissioner of Infrastructure Protection's Approval of Security Plan 16
Application for Commissioner's Approval of Amendment of Approved Security Plan before the completion of specified works 21
Application for Commissioner's Approval of Certificate of Works Completion 21
Audits and Enforcement 22
List of Abbreviations 23

INTRODUCTION

1. Global terrorism is on the rise and Singapore is facing our highest threat of terror in recent years. Buildings which house essential services, are iconic, or with high human traffic, could be targeted by terrorists, with the intent of disrupting such services or inflicting mass casualties.

2. Building security is therefore a key part of our strategy to protect Singapore from terrorist attacks. The Infrastructure Protection Act (**IPA**) establishes a clear regulatory framework to systematically protect Singapore's infrastructure where a successful attack would have disproportionate harm on the public and on Singapore. The IPA also provides more transparency and clarity about building security requirements and processes for building owners and developers.

Objectives of this Document

3. This document sets out statutory requirements for building security mandated under the IPA, which was operationalised on 18 December 2018. It seeks to inform owners and persons responsible ("Responsible Persons" or **RP**) for Special Developments and Special Infrastructures designated under the IPA on the following:
    a. MHA's Security By Design (**SBD**) framework mandated under the IPA and its underlying concepts
    b. Types of developments/infrastructures that will be subjected to MHA's SBD framework, and the procedures by which they will be designated
    c. Regulatory requirements for the submission and approval of Security Plans for Special Developments and Special Infrastructures through MHA's SBD framework

4. Revisions to this document will be issued from time to time. Please check www.police.gov.sg for the latest version. If you have comments or feedback, please send to SPF_CPS@spf.gov.sg.

Structure of this Document

5. This document is divided into the following chapters:

Chapter 1	SBD Framework and the IPA
Chapter 2	Management of Critical Infrastructure under the IPA
Chapter 3	Management of Large/Iconic Infrastructure under the IPA
Chapter 4	SBD Technical Guide

CHAPTER 1 / Security By Design Framework and the IPA

What is Security By Design?

6. The IPA ensures that critical infrastructure, as well as large/iconic buildings are designed with security in mind. In the past decade, MHA has been working with owners of such key infrastructure to take security into account upfront in the development process, by integrating security measures into the building design. This process is known as Security By Design (**SBD**).

7. The key benefit of SBD is that security is effectively incorporated into the building without overly compromising other factors such as the design concept, form and function of the building. It is generally more cost-effective because good design can reduce or even eliminate the need for some security measures. It also avoids costly retrofitting later on.

Who oversees the SBD process?

8. The Commissioner for Infrastructure Protection will oversee the SBD process under the IPA, and is appointed by the Minister for Home Affairs. The Commissioner is supported by the Centre for Protective Security (**CPS**).

How does the SBD process work?

9. Firstly, a security and/or blast consultant is brought on board by the RP to identify the risks and vulnerabilities of a building, and to develop the necessary security measures to mitigate the risks. The security and/or blast consultant must be approved by the Commissioner of Infrastructure Protection as a Competent Person (**CP**) for the project.

10. Secondly, security measures are proposed by the CP to mitigate the relevant security risks as part of the Security Plan to be submitted to the Commissioner for approval. A **localised** and **outcome-based** approach is used to determine the appropriate security measures.

    a. ***Localised –*** SBD process is risk-calibrated and focussed. Protection measures are prioritised on the areas of highest risk.

    b. ***Outcome-based –*** SBD process is flexible. There are different ways to achieve the same security outcome. CPS generally does not prescribe specific risk methodologies or standards, or security measures.

11. Thirdly, CPS works together with the CP and RP to progressively review the various assessment and security reports, in consultation with the respective Government agencies having regulatory oversight or statutory responsibility for the sector ("Sector Lead Agencies"). This is to ensure that the infrastructure is adequately

protected against the identified threat scenarios before formal submission of the Security Plan. This is done concurrently with the rest of the detailed design works for the building.

12. Once the Commissioner has approved the security plan for that infrastructure, building works for that infrastructure may then commence (assuming Provisional or Written Permission from URA has been obtained). All security measures stated in the approved Security Plan must be implemented and maintained.

13. The full details of the SBD process can be found in "Chapter 4: SBD Technical Guide".

What buildings are required to undergo the SBD process under the IPA?

14. MHA will designate two groups of buildings to undergo the SBD process:

    a. First, critical infrastructure, which are vital to the delivery of essential services such as water, power and transport; and

    b. Second, large or iconic buildings, which face a higher level of threat either due to high public footfall, or because of their prominence or symbolic significance.

CHAPTER 2 / Management of Critical Infrastructure (CI) under IPA

1. •Identification of CI by Sector Lead Agency
2. •Designation of CI as Special Development or Special Infrastructure by MHA
3. •CI undergoes SBD review process
   •Approval of Security Plan before commencing construction or major renovation
4. •Implement and maintain security measures in Security Plan
   •Approval of Certificate of Works Completion

Responsibility for security of CI under the IPA

15. Critical infrastructures (CI) are the physical infrastructure and assets that are vital to the continued delivery of the essential services that Singapore relies on, the loss or compromise of which would lead to a debilitating impact on security, economy or public health and safety. CI underpin the functioning of Singapore's society and economy, by enabling the provision of essential services such as food, water, medical care, energy, communications, transportation and banking.

16. A national unity of effort is needed to strengthen the security of CI against physical threats. Although the Government has a role in the protection of CI, owners/operators of CI will also need to be responsible for the security of their own assets and the continuity of their business. These efforts should seek to reduce vulnerabilities, minimise consequences, identify and mitigate threats, and hasten response and recovery efforts related to CI.

17. The person responsible for ensuring that security requirements under the IPA are met ("Responsible Person" or **RP**) is determined based on the legal entity having control and management of the premise the CI is in. This will generally be the owner of the CI. Where the CI has more than one owner, all its owners are collectively known as the RP.

18. However, in cases where the CI is housed in a premise that is not owned by the operator of that CI (e.g. leased data centres), the RP will be the operator of the CI and not the premise owner. Where the CI has more than one operator, all its operators are collectively known as the RP.

Identification of CI

19. CI are primarily identified by the Sector Lead Agencies, in consultation with the RP for the CI.

20. Companies providing essential services should regularly consult their respective Sector Lead Agencies on whether any planned developments or existing infrastructure would be identified as a CI. Failure to identify a CI early may result in downstream delays to its development timeline, if security considerations cannot be factored in the SBD process during the building design phase.

Designation of CI as Special Development / Special Infrastructure

21. MHA will inform the RP for the CI in writing that their CI will be designated as a Special Development (if the CI has not been built or is in the process of being built), or as a Special Infrastructure (if the CI has already been built). This applies to all existing CI and new CI identified in the future. For security reasons, information on which buildings are CIs and designated as Special Developments or Special Infrastructure is restricted to RPs, Sector Lead Agencies and security agencies.

22. Where the premise of a CI is solely owned by the RP, the entire CI's premise will be designated as a Special Development / Special Infrastructure as a whole. This will allow the security of the entire CI to be considered holistically.

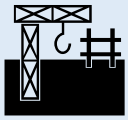
23. Where the CI only occupies part of a larger premise that is not solely owned by the RP (e.g. a data centre in a commercial tenanted facility), only the part of the premise that the CI occupies will be designated as a Special Development / Special Infrastructure.

24. In the rare scenario where there are two or more CIs sharing the same premise, MHA will work together with the relevant RPs to determine the appropriate boundaries that would be consistent with the extent of management and control each RP has for their CI. Similarly, for large-scale CIs that will be constructed over multiple phases, MHA will work together with the relevant RP to phase and align the designation of such CIs as Special Development / Special Infrastructure to the various stages of development where possible, based on the extent of management and control each RP has for their CI.

Requirement to submit Security Plan for approval

25. Once designated as a Special Development or Special Infrastructure, it will be a **legal requirement for the RP to submit a Security Plan to the Commissioner of Infrastructure Protection for approval, before specified works can be carried out**:
    a. CI that are yet to be built / in the midst of construction (designated as Special Developments) will be required to obtain Commissioner's approval for the Security Plan before commencing construction;

b. Existing CI (designated as Special Infrastructure) will be required to obtain Commissioner's approval for the Security Plan before commencing any major renovation works.

 **Critical Infrastructure yet to be built / in the midst of construction**	 **Existing Critical Infrastructure**
• Designated as "Special Developments" • Obtain approval for Security Plan before starting construction works* **Construction works refer to any works for or affecting the foundation, retaining structure, substructure or superstructure of any building/structure (whether temporary or permanent) to be constructed.*	• Designated as "Special Infrastructure" • Obtain approval for Security Plan before starting any major renovation works, including any extension to the existing building/structure • Major renovation works refer to i. In the case of any part of a building/structure containing a critical asset, or is a public place or is accessible to vehicles or vessels, any alteration, extension, repair, dismantling or demolition works carried out to the structure or glazing of that part ii. Any installation or relocation of a critical asset in the premises iii. Any alteration, extension, dismantling or demolition works affecting the perimeter of the premises *[Major renovation works generally do not include insignificant or superficial building works such as painting, erection of internal partitions, landscaping works.]*

26. In instances of major renovations, the Security Plan may be required to cover areas outside of the specified works, so that security risks to the designated premises may be addressed adequately. The scope of such security measures will be based on practical considerations, such as to install or upgrade access control or video surveillance systems.

27. Further details on the Security Plan approval process may be found in Chapter 4: "SBD Technical Guide".

28. Carrying out, causing or allowing the carrying out of any specified works for a Special Development or Special Infrastructure, without approval of Security Plan

by the Commissioner is an offence under the IPA. If convicted, the penalty is a fine not exceeding $200,000 or imprisonment for a term not exceeding 2 years, or both.

29. In addition, the Commissioner may direct the RP to stop any specified works and take actions to comply with the requirement to submit a Security Plan for approval.

30. The requirement to obtain Commissioner's approval for the Security Plan before starting specified works is also incorporated in URA's conditions when applying for Provisional or Written Permission to carry out works.

31. **RPs should inform CPS of upcoming specified works as early as possible**, such as during the project's concept design stage. The earlier CPS is brought on board, the more support CPS will be able to provide during the conduct of the risk assessments and development of the Security Plan. Such support includes advice on the scope of the security review, site selection and the security considerations based on the preliminary design concept of the building.

Requirement to implement and maintain measures in Security Plan

32. After the Commissioner of Infrastructure Protection approves the Security Plan, works can begin (assuming Provisional or Written Permission from URA has been obtained). The security measures in the approved Security Plan must be implemented. The approved Security Plan will specify the implementation schedule for security measures:

    a. **Security measures that are required to be implemented before or upon the completion of specified works**. Upon the completion of specified works, the RP is required to submit a Certificate of Works Completion (CWC) to the Commissioner for approval. The CWC certifies that required security measures have been implemented by the time specified works are completed.

        i. If the specified works require a Temporary Occupation Permit (TOP) or Certificate of Statutory Completion (CSC) from the Building and Construction Authority (BCA), these cannot be obtained without a CWC.
        ii. If the specified works do not require a TOP or CSC from BCA, the CWC must be submitted within 14 days after the completion of specified works.

    b. Security measures that are required to be implemented after the Commissioner's approval of the CWC. The remaining security measures must be implemented in accordance to the schedule set out in the Security Plan.

33. After the CWC is approved, a Special Development becomes a Special Infrastructure and the approved Security Plan of the Special Development becomes the approved Security Plan of the Special Infrastructure. The RP must then maintain every security measure that is implemented under the approved

Security Plan, in order to ensure the operational effectiveness of every security measure.

34. Further details on the CWC approval process and requirements may be found in Chapter 4: "SBD Technical Guide"

35. Failing to implement or maintain every security measure under an approved Security Plan is an offence under the IPA. If convicted, the penalty is a fine not exceeding $20,000 or imprisonment for a term not exceeding 2 years, or both. In the case of a continuing offence, a further fine not exceeding $1,000 for every day during which the offence continues after conviction will be imposed.

36. In addition, the Commissioner may direct the RP to take actions to rectify non-compliance with the approved Security Plan.

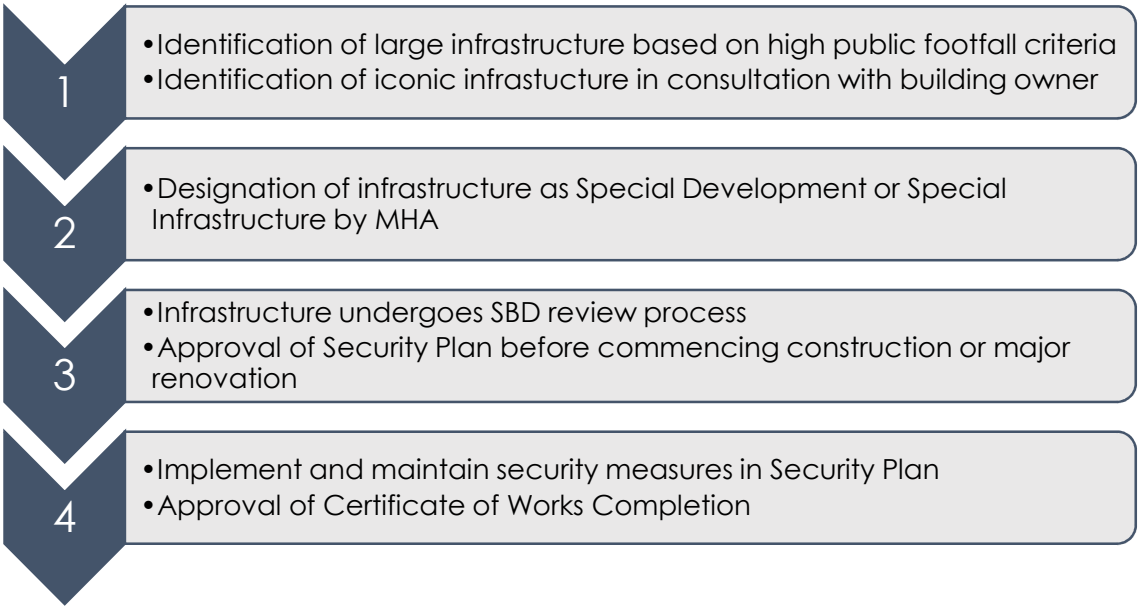
Notification of change in RP of CI

37. Where there is a change in the legal ownership / occupation of a CI that is designated as a Special Development or Special Infrastructure, the person who was the original RP before the change in ownership / occupation is required to inform CPS within 7 days of the change in ownership, through the submission of a notification form found on https://www.police.gov.sg/about-us/organisational-structure/staff-departments/centre-for-protective-security.

Cessation of CI as Special Development and Special Infrastructure

38. A CI will cease to be a Special Development or Special Infrastructure when the Minister cancels its designation by written notice to the RP. This may happen when the premise is demolished, decommissioned or the CI is relocated. The RP of the Special Development or Special Infrastructure should inform CPS once there are plans to demolish, decommission or relocate the CI via SPF_CPS_IPA@spf.gov.sg.

CHAPTER 3 / Management of Large/Iconic Infrastructure under the IPA



Responsibility for security of large/iconic infrastructure under the IPA

39. Building owners have the primary responsibility for protecting their own buildings, including a duty of care to take steps to protect people that work, use, or visit their building from a range of foreseeable threats, including terrorism. The reputation of building owners will result in serious and permanent damage if priority is not given to protecting people against attack. Reputational damage can also have a significant impact on businesses' finances.

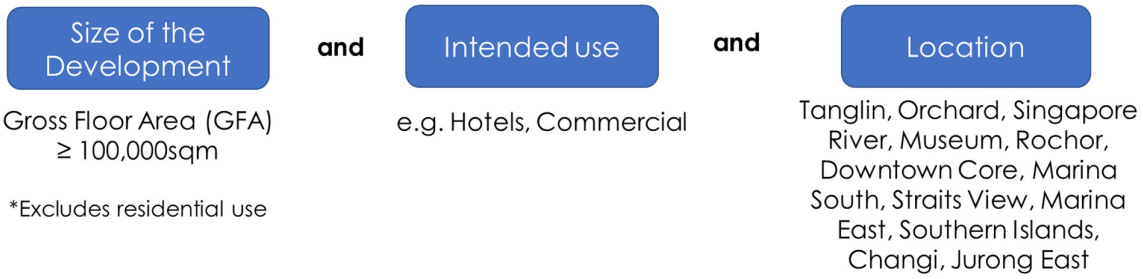
40. For certain buildings, the risk and impact of an attack are much more significant. Large or iconic buildings face a higher level of threat due to high public footfall, or because of their prominence or symbolic significance. In these cases, it is in the public interest to ensure that appropriate security measures are put in place to safeguard lives and property.

41. Under the IPA, the owners of large/iconic infrastructure will be responsible for ensuring that security requirements under the IPA are met ("Responsible Person" or **RP**). This is determined based on the legal entity having control and management of the infrastructure. Where there is more than one owner, all its owners are collectively known as the RP.

Identification of large/iconic infrastructure

42. Large buildings will primarily be identified based on the following three criteria which serve as objective proxies for a development's capacity to attract large crowds due to high public footfall – namely the size of the development (in terms

of gross floor area), its intended use (based on URA's approved use) and its location (based on URA's Planning Areas):



43. Developers and building owners who are unsure whether their buildings meet the criteria may contact CPS for clarification at SPF_CPS@spf.gov.sg.

44. Other developments/buildings that do not meet the criteria in para 42 may also be designated by the Minister for Home Affairs as SD/SI. This includes large / iconic developments/buildings, such as those of symbolic significance to Singapore. Such buildings will be identified as early as possible in the pre-development phase, in consultation with the developer or building owner.

Designation of large/iconic infrastructure as Special Development / Special Infrastructure

45. All large developments that are yet-to-be-built and meet the high public footfall criteria published as a designation order in the Singapore Government *Gazette*[1], are deemed by that designation order to be "Special Developments" under the IPA. This will include all new developments that start / proposed to start construction on or after 1 January 2020.

46. For existing large buildings that meet the high public footfall criteria, they will also generally be designated as Special Infrastructures. MHA will engage each owner and assess the need for security measures, taking into consideration the building's actual land use and profile. MHA will inform building owners of the designation in writing.

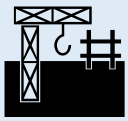
47. MHA may also designate yet-to-be-built and existing developments that do not meet the high public footfall criteria, but are iconic, as Special Developments / Special Infrastructure. Developers will be informed of MHA's intention to designate such iconic developments in writing, as early as possible.

48. Where there are multiple RPs for different parts of the Special Development or Special Infrastructure, MHA will work together with all relevant parties to determine the appropriate boundaries that would be consistent with the extent of management and control each RP has for their part of the building.

[1] The Singapore Government Gazette is a daily publication which carries legal and other statutory notices of general interest for circulation.

Requirement to submit Security Plan for Approval

49. Once designated as a Special Development or Special Infrastructure, it will be a **legal requirement for the RP of large/iconic buildings to submit a Security Plan to the Commissioner for Infrastructure Protection for approval, before specified works can be carried out**:
    a. Developments that are yet to be built / in the midst of construction (designated as Special Developments) will be required to obtain Commissioner's approval for the Security Plan before commencing construction;
    b. Existing buildings (designated as Special Infrastructures) will be required to obtain Commissioner's approval for the Security Plan before commencing any major renovation works.

 **Large/Iconic Developments yet to be built / in the midst of construction**	 **Existing Large/Iconic Buildings**
• Designated as "Special Developments" • Obtain approval for Security Plan before starting construction works* **Construction works refer to any works for or affecting the foundation, retaining structure, substructure or superstructure of any building/structure (whether temporary or permanent) to be constructed.*	• Designated as "Special Infrastructure" • Obtain approval for Security Plan before starting any major renovation works, including any extension to the existing building/structure • Major renovation works refer to i. In the case of any part of a building/structure containing a critical asset, or is a public place or is accessible to vehicles or vessels, any alteration, extension, repair, dismantling or demolition works carried out to the structure or glazing of that part ii. Any alteration, extension, dismantling or demolition works affecting the perimeter of the premises *[Major renovation works generally do not include insignificant or superficial building works such as painting, erection of internal partitions, landscaping works.]*

50. In instances of major renovations, the Security Plan may be required to cover areas outside of the specified works, so that security risks to the designated premises may be addressed adequately. The scope of such security measures will be based on

practical considerations, such as to install or upgrade access control or video surveillance systems.

51. Further details on the Security Plan approval process may be found Chapter 4: "SBD Technical Guide"

52. Carrying out, causing or allowing the carrying out of any specified works for a Special Development or Special Infrastructure, without the approval of Security Plan by the Commissioner is an offence under the IPA. If convicted, the penalty is a fine not exceeding $200,000 or imprisonment for a term not exceeding 2 years, or both.

53. In addition, the Commissioner may direct the RP to stop any specified works and take actions to comply with the requirement to submit a Security Plan for approval.

54. The requirement to obtain Commissioner's approval for the Security Plan before starting specified works is also incorporated in URA's conditions when applying for Provisional or Written Permission to carry out works.

55. **RPs should inform CPS of upcoming specified works as early as possible** (such as during the project's concept design development stage). The earlier CPS is brought onboard, the more support CPS will be able to provide during the conduct of the risk assessments and development of the Security Plan. Such support includes advice on the scope of the security review, site selection and the security considerations based on the preliminary design concept of the building.

Requirement to implement and maintain measures in Security Plan

56. After the Commissioner of Infrastructure Protection approves the Security Plan, works can begin (assuming Provisional or Written Permission from URA has been obtained). The security measures in the approved Security Plan must be implemented. The approved Security Plan will specify the implementation schedule for security measures:

    a. **Security measures that are required to be implemented before or upon the completion of specified works**. Upon the completion of specified works, the RP is required to submit a Certificate of Works Completion (CWC) to the Commissioner for approval. The CWC certifies that required security measures have been implemented by the time specified works are completed.

        i. If the specified works require a Temporary Occupation Permit (TOP) or Certificate of Statutory Completion (CSC) from the Building and Construction Authority (BCA), these cannot be obtained without a CWC.
        ii. If the specified works do not require a TOP or CSC from BCA, the CWC must be submitted within 14 days after the completion of specified works.

b. **Security measures that are required to be implemented <u>after the Commissioner's approval of the CWC</u>.** The remaining security measures must be implemented in accordance to the schedule set out in the Security Plan.

57. After the CWC is approved, a Special Development becomes a Special Infrastructure and the approved Security Plan of the Special Development becomes the approved Security Plan of the Special Infrastructure. The RP must then maintain every security measure that is implemented under the approved security plan, in order to ensure the operational effectiveness of every security measure.

58. Further details on the CWC approval process and requirements may be found in <u>Chapter 4: "SBD Technical Guide".</u>

59. Failing to implement or maintain every security measure under an approved Security Plan is an offence under the IPA. If convicted, the penalty is a fine not exceeding $20,000 or imprisonment for a term not exceeding 2 years, or both. In the case of a continuing offence, a further fine not exceeding $1,000 for every day during which the offence continues after conviction will be imposed.

60. In addition, the Commissioner may direct the RP to take actions to rectify non-compliance with the approved Security Plan.

Notification of change of RP of large/iconic infrastructure

61. Where there is a change in the legal ownership of a large/iconic building that is designated as a Special Development or Special Infrastructure, the person who was the original RP before the change in ownership is required to inform CPS within 7 days of the change in ownership, through the submission of a notification form found on https://www.police.gov.sg/about-us/organisational-structure/staff-departments/centre-for-protective-security.

Cessation of large/iconic infrastructure as Special Developments and Special Infrastructure

62. A development or building will cease to be a Special Development or Special Infrastructure when the Minister cancels its designation by written notice to the RP. This may happen when the premise is demolished or decommissioned. The RP of the Special Development or Special Infrastructure should inform CPS once there are plans to demolish or decommission the development or building via SPF_CPS_IPA@spf.gov.sg.

SBD Overview and Timeline

63. The SBD review process adopts a risk management approach. Risk management is the process of:
    a. identifying critical assets to be protected and their vulnerabilities;
    b. identifying threat scenarios; and
    c. assessing the risks and prioritising the mitigation measures to reduce the risks to an acceptable level.

64. The typical SBD timeline is shown in Fig 1 below:

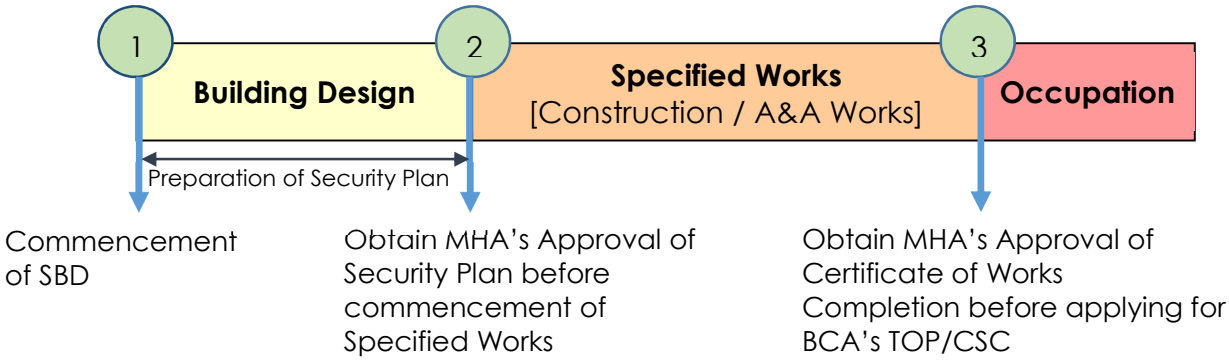


Fig. 1 Submission timeline

65. The SBD process is carried out concurrently with the detailed building design. As the SBD process is outcome-based, our experience with past projects is that the SBD process can be integrated seamlessly with the building design process, especially if security considerations are incorporated early into the design. Based on previous projects, the preparation and approval of Security Plan under the SBD process will take about 9 to 12 months to complete[2], in parallel with the other design works for that infrastructure.

66. Generally, CPS will take about **15 working days** to process each iteration of submitted replies and reports (see para 73 for the reports to be submitted). To avoid delays to the SBD process, the RP should respond to CPS' clarifications within 10 working days. The RP will have to inform CPS if extension of time is required. The number of iterations taken for each report depends on the quality and standard of report submitted. After CPS has cleared all the reports, the RP may submit the application to seek the Commissioner of Infrastructure Protection's approval for Security Plan. We require **20 working days** to process the approval application before issuing the approval letter.

[2] For projects that need to develop structural hardening measures. For developments that do not need to develop structural hardening measures, the SBD process can be shorter. Excludes time taken to hire security/blast consultants

67. It is a legal requirement for the RP to obtain the Commissioner of Infrastructure Protection's approval for the Security Plan before beginning Specified Works. The following steps set out the application workflow.

Step 1: Security Clearance

68. All personnel involved in the SBD process must undergo security screening by MHA, before they can access sensitive project information. This will include the Competent Person (described in Step 2), and may also include senior management and project managers. Due to the confidential nature of the review, the RP should safeguard information related to the review process and limit the number of personnel involved on a strict need-to-know basis.

Step 2: Appointment of Security and/or Blast consultant as Competent Person

69. Security Plans submitted to the Commissioner of Infrastructure Protection must be prepared by a security and/or blast consultant that is approved by the Commissioner to be a Competent Person (**CP**). Please refer to Annex A for requirements for the CP. The role of the CP is to develop effective security solutions against a list of threats provided by MHA, in order to meet the security objectives set out for the Special Development / Special Infrastructure. This will involve carrying out risk assessments, and integrating security planning and solutions into the building's overall design, by working closely with the other project consultants to achieve optimal security solutions. RPs should identify a suitable security and/or blast consultant and his team and submit an application for the approval of CP to CPS **early** in the concept design development stage of the Special Development / Special Infrastructure.

70. The CP will be required to apply evidence-based, tested, and internationally proven methodologies on possible threat scenarios to derive the risk factors. The CP is also responsible for incorporating the RP's inputs, including constraints, preferences, operational/functional requirements, decisions made etc., into the required reports before they are submitted for CPS's review.

Who may be appointed as a CP?
• CPs may be commercial or in-house security and/or blast consultants. The CP (Security) shall be the main security consultant responsible for the SBD review. If blast-related assessments are required, the RP shall appoint another CP (Blast) to carry out the blast-related assessments, who may or may not be the same CP (Security). • The Commissioner will make an assessment of the CP for each project, after assessing the person's relevant qualifications, past experience with SBD projects and the nature of the project.

- CPs need to be approved by the Commissioner of Infrastructure Protection on a per-project basis as some projects may require special expertise, or may be of a sensitive nature.

How should RP assess and select Security and/or Blast consultants?

- RPs should select a security and/or blast consultant based on the requirements and scope of their project. RPs may consider the following factors in assessing and selecting security/blast consultants:
  - Education, qualification, skills and experience
  - Referee reports
  - Professional association and affiliations
  - Previous experience conducting security reviews
  - Relevant subject matter knowledge
  - Impartiality of advice (consider any commercial affiliations)
  - Published professional work

Step 3: Arrange SBD Kick-off Meeting

71. RPs may arrange a kick-off meeting with CPS to share about your project and for CPS to share our requirements.

72. The RP will be informed of the assessed risk profile at the designation of the Special Development / Special Infrastructure. Based on the risk profile, the RP will determine the security objectives specific to the Special Development / Special Infrastructure, that will set the direction of the development of the Security Plan.

    a. In the case of CI, this will involve identifying the critical assets and the minimum service level of the CI.

    b. In the case of large/iconic infrastructure, this will involve identifying areas of mass congregation that need to be protected.

What are Critical Assets?

- Critical Assets are any facilities, systems or equipment which, if damaged or destroyed, may have a debilitating impact on the functioning of the premises. For example, these may include power generators, Air Handling Units (AHUs), telecommunications switches etc.
- RP are responsible for identifying and assessing critical assets for their own Special Developments and Special Infrastructure. In the case of CIs, RP should also consult the relevant Sector Lead Agency regulating or overseeing the CI when identifying the Critical Assets for the CI.

Step 4: Submission of Security Plan

73. The CP will have to prepare up to four reports - Threats, Vulnerability and Risk Assessment (TVRA), Blast Effect Analysis (BEA), Structural Resiliency Study (SRS) and Security Protection Plan (SPP). These reports are collectively referred to as the Security Plan in the IPA.

TVRA and BEA reports

a. When the building's design and structural systems are being developed, the CP shall work closely with the relevant persons to incorporate sensible security design practices to minimise security risks to the critical assets. Please refer to Annex B for a description of Key Building Design Considerations. The CP will have to consider the functional needs of the building and the operational requirements of the RP. In the case of CI, this will include safe spaces[3] to protect essential personnel needed for the continued functioning of the facility.

b. The CP shall be required to carry out a risk assessment of the building to determine the risks to the critical assets, with the findings included in the TVRA. The TVRA should consist of an introduction of the Facility, including the purpose, nature of its business and how it functions, a list of critical assets supporting the operations, its location and layout, existing/baseline security measures and its ranked security objectives. Please refer to Annex C for requirements for the TVRA.

c. Where the vulnerabilities of structural elements against explosive loads need to be studied in order to determine the risks, the CP will identify the affected structural elements and conduct a BEA to determine their adequacies. Please refer to Annex D for Requirements for BEA. BEA reports are not required for selected Special Developments or Special Infrastructure that do not need structural hardening.

d. The TVRA and BEA reports have to be prepared in consultation with the RP and submitted concurrently to CPS. After the submission of any report, the CP will support the RP by providing any necessary clarifications and justifications. The review may be carried out over a few iterations and the RP has to go through the CP's reports, clarifications and agree on the risk assessment and the prioritisation of critical assets to be protected based on the risk scoring.

e. The CP is to update the reports with the necessary amendments, clarifications and supporting information after the reports have been accepted.

[3] Safe spaces are hardened spaces for short-term, small group protection.

a. The CP shall recommend in the SPP a comprehensive suite of security measures to address **all** the risks, as determined from the risk assessment, to fulfil the stated security outcome, with the exact combination of structural/physical, operational and technological measures to be calibrated according to the risks posed by the various threat scenarios and the criticality of the assets in question. The CP shall:

    i. Rank the recommended security measures in terms of the risk consequence and priority, highlighting the security measures that must be implemented; and
    ii. Illustrate the reduction of risk achieved in each case by updating the risk levels contained within the risk assessment, should the recommended measures be implemented.

b. For structural elements that are concluded in the BEA to be inadequately protected, and if the security solution requires structural hardening/enhancement, the CP shall prepare and submit the SRS, supporting the CP's recommendations for structural hardening measures to mitigate relevant vulnerabilities and risks identified in the risk assessment with the analysis carried out in accordance with the requirements stipulated in Annex D. The CP will design the structural elements based on validated approaches. SRS reports are not required for selected Special Developments or Special Infrastructure that do not need structural hardening.

c. The security measures proposed by the CP must comply with prevailing statutory requirements, codes or guidelines published by government authorities. This includes, but is not limited to URA's development control parameters, BCA's Building Code, SCDF's Fire Safety Code, and/or other relevant international codes such as the International Ship and Port Facility Security (ISPS) Code.

d. The CP will have to work with the RP's appointed representatives and Qualified Persons (QPs) to incorporate the final security measures into relevant project plans.

e. Should certain security specifications or designs require amendments, the CP will carry out the necessary amendments, incorporate the necessary revisions to the original analysis to all relevant reports and submit the revised reports for the RP's approval.

f. The RP must then select the final set of protection measures, after making the trade-offs between security and other considerations, such as cost, operational effectiveness and aesthetics. This involves determining and acknowledging the level of risk (i.e. residual risk) which remains after measures have been put in place. This should be done in consultation with CPS.

g. The decision by the RP on the final set of protection measures and acceptance of residual risks [4] (and associated responsibility) must be deliberated and endorsed in writing by a sufficiently senior representative (e.g. Emergency Planning Officer (**EPO**) or Chief Executive). This is to be done in consultation with the Sector Lead Agency.

h. The SPP should also include all the necessary details for the implementation of the security measures, including security design features that had been developed from the TVRA, BEA and SRS, and all necessary certifications, test data, calculations and drawings relevant to the Facility. A Summary Table of the Mitigation Measures (SMM) to be implemented is to be included in the SPP report submitted. The SMM should include a schedule specifying the implementation schedule for security measures, covering:

   i. Security measures that are required to be implemented before or upon the completion of specified works; and

   ii. Security measures that are required to be implemented after the Commissioner's approval of the CWC, following the completion of specified works.

i. For detailed requirements for SPP, please refer to Annex E.

j. The SRS and SPP can be submitted concurrently to CPS. CPS will give our comments, if any, to the RP. The RP and CP have to address these comments and propose amendments, if required. The review may be carried out over a few iterations and the RP has to go through the CP's reports, clarifications and agree on the protective measures to be adopted.

k. Finally, the CP is to update the reports with the necessary amendments, clarifications and supporting information after the reports have been accepted.

How to minimise delays to the SBD process?
To minimise delays, RPs can: - • Engage a security and/or blast consultant early to work with the project architects and engineers to incorporate security considerations upstream in the design; • Proactively manage the security and/or blast consultants and vet the security reports carefully before sending them to CPS for review; • Provide clear guidance to the security and/or blast consultants on key decisions such as critical assets and security measures to be adopted; • Avoid major changes to the building design midway through the security review; • Take an active role to ensure that the CP addresses queries raised by CPS in a timely and complete manner; and • Adopt the templates for the reports provided by CPS and the requisite analysis method.

[4] Residual risk is defined as the risk that could not be fully mitigated despite putting in all measures and controls.

Step 5: Application for Approval of Security Plan

74. When CPS has no further comments to the TVRA, BEA, SRS and SPP (collectively termed as "Security Plan") for designated Special Developments or Special Infrastructures, the RP can proceed to submit the application for Approval of Security Plan found on https://www.police.gov.sg/about-us/organisational-structure/staff-departments/centre-for-protective-security. The application must be accompanied with the finalised Security Plan and such other documents that may be required by the Commissioner.

75. Upon approval, the Security Plan will be termed as the approved Security Plan. CPS's approval of the Security Plan will be included as a condition for URA's approval of Written Permission for any development application submitted to URA under the Planning Act.

Application for Commissioner's Approval of Amendment of Approved Security Plan before the completion of specified works

76. The RP or the Commissioner may at any point in time request for amendments to the approved Security Plan. Depending on the scope of the amendments, revisions to the TVRA, BEA, SRS and SPP may be necessary. Once the Commissioner approves the amended Security Plan, the previous approval of the Security Plan will be superseded by the current approval.

Application for Commissioner's Approval of Certificate of Works Completion

77. Upon the completion of specified works, the RP is required to submit a Certificate of Works Completion (CWC) to the Commissioner for approval. Before the application for CWC may be considered, the RP shall request for a joint site inspection with CPS of the completed specified works. The CWC certifies that the required security measures in the Security Plan have been implemented by the time specified works are completed. The RP is required to work with the CP to ensure the following:

Step 1: Supervise implementation of security measures during specified works

78. The CP is required to oversee specified works (whether construction or major renovation) to ensure that all the security measures are implemented as spelt out within the SPP. This includes overseeing the supply, deployment, construction, installation, testing and commissioning of the security measures/systems, and ensuring that these measures/systems are implemented according to the technical specifications and standards.

Step 2: Documentation

79. The CP must verify that the method statements, shop drawings, materials and workmanship specifications submitted by the vendor/contractor are in accordance with the specifications of the construction tender as awarded. If the contractor proposes any deviation from the security measures as spelt out within the approved Security Plan, the CP shall advise the RP whether the deviation is acceptable.

Step 3: Assess changes to Approved Security Plan (if any)

80. The RP shall update CPS if there are changes to the approved Security Plan, such as unforeseen site issues or operational constraints during construction. The RP has to ensure that these changes will not lead to a lower level of protection for the critical processes and assets specified in the approved Security Plan. CPS will determine whether there is a need to re-assess the new security risks and to seek Commissioner of Infrastructure Protection's approval for the amendments to the approved Security Plan accordingly. If not, the applicant may proceed to Step 4.

Step 4: Submission of CWC

81. The RP shall submit the application for approval of CWC with the necessary supporting documents to show that measures have been implemented as required in the approved Security Plan. The supporting documents may include, but are not limited to, the summary table of mitigation measures, test certifications, etc. For security measures that will be implemented only after the Commissioner's approval of the CWC (e.g. security manpower deployment), the RP should provide an indicative implementation date in the CWC.

    a. If the specified works require a Temporary Occupation Permit (TOP) or Certificate of Statutory Completion (CSC) from the Building and Construction Authority (BCA), these cannot be obtained without an approved CWC.

    b. If the specified works do not require a TOP or CSC from BCA, the CWC must be submitted within 14 days after the completion of specified works.

Audits and Enforcement

82. Special Developments / Special Infrastructures may be randomly selected by CPS to be audited to ensure that security measures stated in the approved Security Plan and approved CWC are implemented, or maintained to be in good working condition.

83. If there are any deviations from the approved Security Plan or approved CWC, the Commissioner may direct the RP in writing to take the necessary steps to rectify such deviations.

List of Abbreviations

A&A	Addition and Alteration
BCA	Building and Construction Authority
BEA	Blast Effect Analysis
CI	Critical Infrastructure
CP	Competent Person under the Infrastructure Protection Act
CPS	Centre for Protective Security
CSC	Certificate of Statutory Completion (from BCA)
CWC	Certificate of Works Completion
EPO	Emergency Planning Officer
IPA	Infrastructure Protection Act
MHA	Ministry of Home Affairs
RP	Responsible Person under the Infrastructure Protection Act
SBD	Security By Design
SD	Special Development
SI	Special Infrastructure
SPP	Security Protection Plan
SRS	Structural Resiliency Study
TOP	Temporary Occupation Permit (from BCA)
TVRA	Threats, Vulnerability and Risk Assessment
URA	Urban Redevelopment Authority