



[Home](#) > [Media room](#) > [Newsroom](#) >

Second Reading of the Infrastructure Protection Bill 2017 - Speech by Mrs Josephine Teo, Minister,...

Parliamentary Speeches

## Second Reading of the Infrastructure Protection Bill 2017 - Speech by Mrs Josephine Teo, Minister, Prime Minister's Office, Second Minister for Home Affairs and Second Minister for Manpower

2 October 2017

This article has been migrated from an earlier version of the site and may display formatting inconsistencies.

1. Mr Speaker, I beg to move, "That the Bill be now read a second time".

### **Terrorists Target Crowded Places and Iconic Buildings**

2. Members of the House will be aware, as it appears on the order paper, that the honourable member Mr Christopher De Souza has filed a motion on fortifying Singapore's resolve against the rising threat of terrorism. This Bill is also about fortifying Singapore, specifically to protect our critical infrastructures and certain buildings.

3. Today's terrorists typically target crowded places or iconic buildings, so that they can take out as many lives as possible, and make a huge statement with their acts. Their aim is to create fear, and upend our way of life in the ideological battle between their and our values. There are already many horrifying attacks:

In August this year, vehicle-ramming attacks in Catalonia, Spain killed 16 people. The terrorists behind the attacks had also planned to bomb iconic buildings in Barcelona.

In 2011, a car bomb exploded in front of government buildings in Oslo, which included the Prime Minister's office. It killed eight people and significantly damaged several buildings.

In 2008, the Marriott Hotel in Islamabad was targeted by a massive truck bomb. It was stopped by the hotel's vehicle security barrier 40 metres from the front of the hotel, which blunted the attack. But it was not enough; the blast left a huge crater outside the hotel and 54 people dead.

### **Response Needed**

4. These incidents testify to the importance of adequately protecting our infrastructure. Despite heightened alert and best efforts by the security agencies, the attacks had still succeeded to varying degrees.

5. Singapore is not immune to such threats. We have been cited as a target in jihadist publications and videos. Attacks have been plotted against us, such as the one involving Marina Bay Sands last year. There has been a significant rise in the number of radicalised

individuals detained. Terrorist attention on this region is also growing, fuelled by conflict in areas like Marawi.

6. Realistically, we cannot expect to uncover and foil every terrorist plot. That is why our response has to be comprehensive, covering not just pre-emptive action by the security agencies, but infrastructure protection as well, to mitigate the consequences of a successful attack.

7. Over the past two years, the Government has expanded CCTV coverage, enhanced border protection, upgraded the response capabilities of our security forces, and mobilised the community, among other measures. The Public Order Act was amended in April to require organisers of large-scale events to take necessary security measures to protect the public.

8. This Bill is a continuation of our counter-terrorism efforts. It has to be seen against the backdrop of the evolving and worsening threat, and the cognisance that no single approach can effectively deal with it. The Bill aims to protect key infrastructure against attacks. Indeed, measures like vehicle barriers, and hardening of structures and of glazing, are a key line of defence. They can both deter attacks, and blunt the force of an attack. They can save lives.

### **Why Regulate Infrastructure Protection**

9. Building security is the responsibility of building owners, and it will remain so. They know their needs and operations best, and are responsible for the safety of their tenants and the public who visit their buildings.

10. But for certain buildings, the risk and impact of an attack are much more significant, for example those with high public footfall, or are iconic of our society and way of life. In these cases, it is in the public interest for the Government to be proactive in ensuring that appropriate security measures are put in place to safeguard lives and property.

11. Today, MHA already works with owners of critical infrastructure and selected commercial buildings, to take security into account upfront in the development process, by integrating it into the building design. This is called security-by-design.

12. Current laws, however, do not provide us with the authority to mandate such infrastructure protection; we have relied on engagement and persuasion.

13. While such an approach has worked reasonably well so far, given the worsening threat environment, the Government has assessed that we should establish a clear regulatory framework to more systematically protect Singapore's infrastructure. This will also provide more transparency and clarity about the requirements and processes for building owners and developers.

### **What the Bill is about**

14. The Infrastructure Protection Bill sets out such a legal framework. It aims to achieve three things.

**15. First, the Bill will ensure that critical infrastructure, as well as buildings with high public footfall and iconic buildings, are designed with security in mind.**

16. It is impractical to turn the whole of Singapore into a fortress. In deciding which buildings to regulate, we have to consider the risk to the public, the national interest, and the cost to businesses.

17. A successful strike on critical infrastructure will disrupt essential services – such as power, water or transport. An attack on large buildings with high public footfall could result in mass casualties. Iconic buildings are also attractive targets for terrorists because of their international reputation or significance to Singapore. The Bill will require such infrastructure to undergo a security-by-design process before they are built or renovated.

18. **Second, the Bill will allow the authorities to issue directives and orders to protect other buildings in Singapore against terrorist attacks.** While any building could be a target, it is clearly not practical to require every building in Singapore to undergo security-by-design.

19. For buildings that need not undergo security-by-design, the Bill enables MHA to issue directives for owners to put in place appropriate security measures against the risk of a terrorist attack. If an attack is imminent, emergency orders may also be issued to protect these buildings.

20. **Third, the Bill will enhance powers to protect sensitive locations.** These locations are currently declared under the Protected Areas and Protected Places Act, or PAPPA. Most of them are critical infrastructure or military areas. The Bill will address gaps in the PAPPA. It will give the owners of these locations enhanced powers to address threats and implement heightened surveillance in the area surrounding the facility.

21. I will go through each of these three aspects covered by the Bill in some detail.

### **Benefits of Security-by-Design**

22. Security-by-design is a process to ensure that security is integrated into the building design. It attempts to mitigate security risks through good building design, and incorporates security measures upfront into the building features. Examples of such security measures include:

Hardening of structural elements, such as walls and columns, to resist bomb blast effects;

Providing for a stand-off distance using security barriers to prevent unauthorised vehicles from coming close to the building; and

Combining security technology with operational processes, such as monitoring CCTVs, operating access control systems, or implementing security procedures

23. The key benefit of security-by-design is that security is effectively incorporated into the building without overly compromising other factors such as the 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.

### **Security-by-Design as a Legal Requirement**

24. Security-by-design will be made a legal requirement under the Bill.

Clause 5 will empower the Minister for Home Affairs to appoint a Commissioner of Infrastructure Protection. The Commissioner will be responsible for the administration of the Bill, including security-by-design requirements.

Part 4 of the Bill, or Clauses 32 to 48, details the security-by-design requirements.

In Part 5, Clauses 51 to 53 allow the Commissioner to issue directives to address non-compliance with security-by-design requirements.

### **Designation of Special Developments and Special Infrastructures**

25. The Minister will designate the buildings that need to undergo security-by-design in the interests of public safety and public security, or national interests. Under Clause 34, such new buildings that have not yet been built will be designated as "Special Developments". They will need to undergo security-by-design before construction starts. Under Clause 41, existing buildings will be designated as "Special Infrastructures". They will need to undergo security-by-design when they undertake major renovations.

26. The Minister will designate two groups of buildings as Special Developments or Special Infrastructures:

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

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

27. All critical infrastructures, whether existing or new, will be designated under the Bill. Owners of such infrastructures would already be familiar with security-by-design. In the past decade, MHA has worked closely with Government agencies to identify critical infrastructures and incorporate security into their design. This will continue under the Bill.

28. As for the second group of buildings, new developments that have potential of high public footfall will be designated as Special Developments. They will be identified based on objective criteria such as Gross Floor Area; whether they are zoned for commercial, community or mixed use; and whether they are in certain planning areas. In Clause 34, the Bill makes clear that we will publish the criteria which will be used to designate a class of Special Developments under a Gazette order. The order will require any new developments that meet the criteria to undergo security-by-design.

29. We may also designate new developments that do not meet the high public footfall criteria, but are iconic, as Special Developments.

30. For existing buildings that meet the high public footfall criteria, they will generally be designated as Special Infrastructure. MHA will engage each owner and assess the need for security measures, taking into consideration the building's actual land use and profile. Any further requirements to be imposed will be reasonable and practical, taking into account the fact that these are existing and not new buildings.

31. We will be as transparent as possible about the buildings that we will designate as Special Developments or Special Infrastructures, and inform the building owners as early as we can.

### **Requirement to Submit a Security Plan for Approval**

32. Clause 32 describes who will be the responsible person of a Special Development or Special Infrastructure.

33. After a new development or existing building is designated, Clauses 35 and 42 require responsible persons to submit a security plan to the Commissioner for approval, before specified works can be carried out.

34. The term "specified works" is defined in Clause 2. For Special Developments, specified works refer to key construction works such as those affecting the foundation, retaining structure, substructure or super structure. For Special Infrastructures, specified works refer to an extension of the premises, or major renovation works.

35. Clause 33 explains what the security plan should cover. It should include the risk assessment and necessary security measures for the designated premises, and must be prepared by a competent person approved by MHA.

36. For Special Infrastructures, a security plan to be approved by the Commissioner is required for major renovation works. The term "major renovation" is defined in Clause 2, and broadly refers to works that may introduce new security risks, for example, works at publicly accessible areas, the perimeter, or involving critical assets. A security plan to assess the risks, adjust existing security measures or add new measures, will be required.

37. 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 reasonable, for example, to install or upgrade access control or video surveillance systems.

38. It will be an offence to commence specified works without an approved security plan. The penalty is a fine of up to \$200,000 or 2 years' jail or both.

39. Under Clause 51, the Commissioner may direct the responsible person to stop any specified works and take actions to comply with the requirement to submit a security plan for approval. This requirement will also be incorporated in URA's conditions when granting provisional permission to developers to carry out works.

#### **Requirement to Implement and Maintain Measures in Security Plan**

40. After the Commissioner approves the security plan, works can commence and the security measures in the approved security plan must be implemented. Clauses 38 and 45 describe this.

41. Clauses 39 and 46 require the responsible person to submit a Certificate of Works Completion (or CWC) and obtain the Commissioner's approval. The CWC certifies that required security measures have been implemented by the time specified works are completed. The CWC must be prepared by an approved competent person. Clause 40 explains that Special Developments become Special Infrastructures once the CWC is approved.

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

43. After the CWC is approved, Clauses 40 and 47 require the responsible person to implement the rest of the security measures, and maintain every security measure in accordance with the approved security plan. Failure to do so will be an offence punishable with a fine of up to \$20,000 or 2 years' jail or both.

44. Clauses 38 and 45 allow flexibility through regulations for security measures in the security plan to be modified after the CWC is approved, for example, due to changes in the owner's operational needs, or if existing measures need to be adjusted because of new specified works.

45. Under Clauses 52 and 53, the Commissioner may direct the responsible person to take actions to rectify non-compliance with the approved security plan.

#### **Directives and Orders**

46. The second key aspect of the Bill is the introduction of directives and orders to protect buildings against terrorist attacks.

#### **Security Directives Issued by Commissioner**

47. The Commissioner may issue security directives to Special Developments and Special Infrastructures.

48. Under Clause 54, the Commissioner may direct the responsible person of a Special Infrastructure to implement and maintain specific security measures, if it is necessary to address any security risk. This could be because the Special Infrastructure does not have any approved security plan (meaning that it did not previously undergo security-by-design); or because the approved security plan does not address emerging or new security risks.

49. Under Clause 55, the Commissioner may issue security directives to publicly accessible premises which have not been designated as Special Infrastructures. The purpose is to be able to direct persons to implement specific security measures to address the risk of a terrorist attack. Such measures could include installing vehicle security barriers, or improving CCTV coverage and allowing the Police to view the feeds in order to protect the building against a terrorist attack. These measures will also not

include the strengthening of structural elements against blast effects, which typically involve major structural modifications.

50. Clause 56 makes non-compliance with security directives an offence. For directives under Clauses 49 to 54, which is applicable to Special Infrastructures, this is punishable by a fine of up to \$100,000 or imprisonment of up to 2 years or both. For directives under Clause 55, which is applicable to buildings not designated as Special Infrastructure, this is punishable by a fine of up to \$50,000 or imprisonment of up to 2 years or both. It is also an offence if the person continues not to comply with the security directive even after he is convicted.

51. Security directives are intended as a last resort. Where a building is assessed to be at risk, MHA and the Police will first engage building owners to develop practical security measures and encourage them to undertake those measures voluntarily. But if the building owner is resistant and there is a potential risk to public safety and security, directives will be used.

### **Minister's Orders to Address Imminent Threats**

52. To address any imminent risk of a terrorist attack, Clause 58 empowers the Minister to issue an order to any premises to take immediate actions against that risk.

53. The order can require security measures such as preparing and implementing contingency plans, installing temporary security measures, and deploying security guards to restrict access of people and vehicles.

54. The order can also require the temporary closure of a part or the whole of the premises, allowing state forces to access the premises, or for the owner to provide any information relevant to protecting the premises, for example, their building plans, visitor and car park records, or CCTV feeds.

55. Clause 60 makes non-compliance with the Minister's orders an offence, punishable by a fine of up to \$100,000 or 5 years' jail or both. Under Clause 65, if the Minister's order is not complied with, the Commissioner may enter the premises to carry out the directions in the order, and recover the costs from the owners.

### **Appeals**

56. Part 7 provides for appeals to the Minister against certain decisions of the Commissioner. During security-by-design, if the Commissioner rejects the security plan of a Special Development or Special Infrastructure, the responsible person may appeal to the Minister. Persons issued with security directives under Part 5 may also appeal to the Minister. In cases where independent technical advice is needed, the Minister may refer the appeal to an Appeal Advisory Board, comprising relevant experts, and appointed under Clause 63.

### **Enhanced Powers to Protect Sensitive Locations**

57. The third and final key aspect of the Bill is to enhance powers to protect sensitive locations. These are locations currently declared under the Protected Areas and Protected Places Act (or PAPPA). Most Singaporeans would be familiar with the red warning signs. These are sensitive facilities where the movement and conduct of persons need to be controlled for security reasons, for example, border checkpoints, military training camps, and critical infrastructure delivering essential services.

58. The difference between a Protected Area and a Protected Place is that a Protected Place is not accessible to the public without approval from the owner of the place. Let me use the airport as an illustration. The transit facilities are Protected Places. So only persons with a valid boarding pass or other authorisation may enter those places. On the other hand, the departure halls are Protected Areas and are accessible to the general public. But in both locations, the movement and conduct of people are controlled for security reasons.

59. The purpose of the PAPP is to provide powers to authorities in charge of sensitive locations and their guards to protect their premises. The key provisions of the PAPP remains relevant today. The Bill will repeal the PAPP, enhance the provisions, and port them over to Part 3, or Clauses 8 to 31, of this Bill.

60. Most provisions remain unchanged. Protected Areas and Protected Places declared under the current PAPP will remain under the new Act. So will existing powers for guards to control movement in the Protected Area or Place, conduct search of persons and property, remove persons and property, and arrest persons by force if necessary.

61. Clauses 12 and 18 make explicit the responsibilities for authorities in charge of Protected Areas and Places. Where guards are deployed, they must be authorised officers to ensure that they have the proper training and authorisation to exercise the powers. The boundaries of Protected Areas and Places must be clearly marked. For Protected Places, measures must be put in place to prevent unauthorised access.

62. To address today's threat environment, the Bill will make two enhancements to the powers for Protected Areas and Protected Places.

### **Powers to Prevent Unauthorised Photography**

63. The first enhancement is to prevent terrorists from carrying out pre-attack surveillance of their targets. Images of Protected Areas and Places can threaten public safety, if used for unlawful purposes. They can reveal details of security measures, the flow of people and the movement of guards.

64. To address this, Clause 29 will make unauthorised photography of the whole or any part of a Protected Area or Protected Place an offence. This means that photos can only be taken if the authority in charge of the Protected Area or Protected Place gives its permission. This will apply to land-based as well as to aerial photography. Clause 29 also empowers authorised officers to direct persons to stop taking photos and delete any photos taken. Signs will be displayed at the perimeter of the Protected Area or Place to indicate that unauthorised photography is prohibited.

65. Clause 30 deals specifically with photography by unmanned aerial vehicles. Similar provisions exist in the Air Navigation Act and the Public Order Act. Unauthorised photography of Protected Areas and Places by unmanned aerial vehicles is an offence. Authorised officers designated by Police under Clause 30 will have powers to address such instances of unauthorised photography, such as assuming control of the unmanned aerial vehicle to land it safely and quickly.

### **Powers to Secure Surrounding Area**

66. The second enhancement is to deter and detect persons in the surrounding area who pose a security threat to the Protected Area or Protected Place. This could be a person who carries a suspicious bag or parks a truck near the perimeter, or loiters near the Protected Area or Place without good reason. Such persons could be carrying dangerous items. They could also distract the attention of authorised officers.

67. Potential attacks overseas have been stopped by vigilant guards in the surrounding area of a sensitive facility. In April this year, Police in the UK arrested a man near the Prime Minister's office on suspicion of preparing to commit an act of terrorism. It turned out that he was carrying three knives in a rucksack.

68. Clauses 27 and 28 provide authorised officers with powers to identify and deal with potential security threats in the surrounding area. When engaging a person in the surrounding area, authorised officers may request for his personal identification and reason for being there. If the person fails to comply, or does not give a good and lawful reason to be there, the authorised officer may direct him to move on. The authorised officer may also inspect belongings and vehicles, if he reasonably suspects that the person is carrying dangerous items.

69. Clause 26 makes clear that the powers in Clauses 27 and 28 apply only if the surrounding area is specified in the order of the Protected Area or Place. Signs will be displayed at the perimeter of the Protected Area or Place to indicate that the powers apply.

### **Public Consultation**

70. MHA has consulted stakeholders in developing the Bill, including from the built environment sector, such as real estate developers, architects and engineers, as well as owners and operators of critical infrastructure. Security industry professionals were also consulted.

### **Strengthening Expertise and Resources**

71. We recognise that the new infrastructure protection framework would require more expertise and resources in the area of building security.

72. MHA and the Professional Engineers Board will establish a new category of specialist Professional Engineers in Protective Security, or the PE (PS) scheme, to recognise and develop local expertise. It will be launched in 2018. In the longer term, we will consider making the involvement of Professional Engineers in Protective Security in the security-by-design process as a legal requirement.

73. MHA will also publish updated Guidelines for Enhancing Building Security in Singapore. This will guide building owners on conducting security risk assessments, designing secure buildings, and selecting appropriate security measures. The Centre for Protective Security Studies will conduct training and outreach on the guidelines.

### **Conclusion**

74. Mr Speaker, please allow me to conclude my speech in Mandarin.

75. 目前，内政部会就选定的建筑发展项目，同业者一起研究如何在设计中融入保安元素。但是政府至今也只能靠鼓励和劝说来推动这项工作，缺乏法律依据与基础。如今大环境的恐怖威胁越来越紧迫，政府认为有必要建立起一套管制框架，才能更有系统地为新加坡的基础设施提供保障。

76. 这项"基础设施保护法案"(Infrastructure Protection Bill)，将立法规定主要建筑在设计时必须结合保安措施。所谓"主要建筑"，就包括：提供基本民生服务的建筑设施，以及客流量庞大的大规模建筑，或者因为某种象征意义而分外突出的标志性建筑，这些建筑都特别容易成为恐怖份子锁定的目标。

77. 其他建筑，即使不属于"特别基础设施"类别，只要政府认为有一定程度的恐袭风险，政府也有权指示这些建筑落实保安措施。

78. 不过，必须强调的是，基础设施保护措施固然可以有效地减缓恐怖威胁，却无法完全杜绝这股潜在的危险势力。我们必须从各个方面提高警惕，全方位加强戒备。大家必须把这项新法案视为全国反恐框架下的其中一个环节，与全岛增设电眼、边境安保、安全部队应对能力、社区防卫责任等各个环节环环相扣，才能建构起健全的反恐框架。

79. 诚然，恐怖主义的多面向威胁绝对不是单靠任何一项措施或立法就足以解决的。每一个新加坡人都要有所担当，为保障国家的安全和安保尽一份力。

[↑ Back to top](#)

[Who we are](#)

[What we do](#)

[Careers](#)

[Get involved](#)

[Our stories](#)

[Media room](#)

[e-Services](#)

[Reach us](#)



[Contact](#)

[Feedback](#)

© 2026 Government of Singapore, last updated 8 May 2026

[Report Vulnerability](#)

[Privacy Statement](#)

[Terms of Use](#)

[REACH](#)

Made with



Built by

