House of Commons
Transport Committee

UK Transport Security – preliminary report

First Report of Session 2005–06

Report, together with formal minutes, oral and written evidence

Ordered by The House of Commons to be printed 23 November 2005

The Transport Committee

The Transport Committee is appointed by the House of Commons to examine the expenditure, administration, and policy of the Department for Transport and its associated public bodies.

Current membership

Mrs Gwyneth Dunwoody MP (*Labour, Crewe*) (Chairman)
Mr David Clelland MP (*Labour, Tyne Bridge*)
Mr Jeffrey M. Donaldson MP (*Democratic Unionist, Lagan Valley*)
Clive Efford MP (*Labour, Eltham*)
Mrs Louise Ellman MP (*Labour/Co-operative, Liverpool Riverside*)
Mr Robert Goodwill MP (*Conservative, Scarborough & Whitby*)
Mr John Leech MP *(Liberal Democrat, Manchester, Withington*)
Mr Eric Martlew MP (*Labour, Carlisle*)
Mr Lee Scott MP (*Conservative, Ilford North*)
Mr Graham Stringer MP (*Labour, Manchester Blackley*)
Mr David Wilshire MP (*Conservative, Spelthorne*)

Powers

The Committee is one of the departmental select committees, the powers of which are set out in House of Commons Standing Orders, principally in SO No 152. These are available on the Internet via www.parliament.uk.

Publications

The Reports and evidence of the Committee are published by The Stationery Office by Order of the House. All publications of the Committee (including press notices) are on the Internet at www.parliament.uk/transcom. A list of Reports of the Committee in the present Parliament is at the back of this volume.

Committee staff

The current staff of the Committee are Dr John Patterson (Clerk), Annette Toft (Second Clerk), Clare Maltby (Committee Specialist), Philippa Carling (Inquiry Manager), Tony Catinella (Committee Assistant), Miss Michelle Edney (Secretary), Henry Ayi-Hyde (Senior Office Clerk) and Luke Robinson (Media Officer).

Contacts

All correspondence should be addressed to the Clerk of the Transport Committee, House of Commons, 7 Millbank, London SW1P 3JA. The telephone number for general enquiries is 020 7219 6263; the Committee's email address is transcom@parliament.uk

Contents

Report

Summary

Transport systems are particularly vulnerable to terrorist attack. The threat to the UK's transport network was demonstrated tragically by the bombings on London Underground trains and a bus on 7 July, and its continued vulnerability by the further bombing attempts on 21 July. The threat to the network remains high, and all possible measures need to be taken to prevent a repetition of these events. Inadequacies in the present arrangements must be identified and rectified quickly. Parliament must be assured that the arrangements for the protection of the travelling public are in excellent condition.

The committee invited the Secretary of State for Transport, and officials from the Transport Security and Contingencies Directorate of the Department (TRANSEC), to answer questions on the state of protective security on UK transport networks on 2 November. This was a preliminary hearing and, as a result of what we heard then, we have announced an inquiry into aspects of protective security on UK transport networks, with further hearings next year.

Among the issues we examined on the 2 November, and shall be examining further are:

- The level and nature of the threats to UK transport networks

- The process by which protective security is directed by 'threat information'

- Coordination amongst the relevant intelligence and security agencies to support the work of TRANSEC

- Cooperation between the Government and the transport industries to ensure the security of the travelling public

- The resources available to TRANSEC and how it reports its activities publicly

- The role of the public and the news media in ensuring that protective security measures in place are fully effective

A fully functioning transport network is essential to the economic life of the nation. All too often we take this for granted. The events of 7 July have demonstrated that this is no longer an affordable luxury.

1 Introduction

1. As a consequence of the terrorist attack on the World Trade Centre, New York City, and the Pentagon building, Department of Defence, Washington D.C. on 11 September 2001, and subsequent attacks such as the bombings on the railway in Madrid on 11 March 2004, governments around the world have increased their response to the terrorist threat. Still more recent outrages closer to home, the fatal bombings in London on 7 July 2005, and the events of 21 July, have propelled transport security, and the vulnerability of the UK's transport networks to such attacks, into the forefront of British public consciousness.

2. These events, their consequences for the security of the travelling public in the UK and British travellers abroad, and the response of the Government to the continuing threat, provided the reason for our invitation to the Secretary of State for Transport to brief us on what was being done by his Department to protect the British travelling public from terrorist violence.

3. The Transport Security and Contingencies Directorate (TRANSEC) of the Department for Transport regulates UK transport security. TRANSEC's aims are:

> "to protect the travelling public, transport facilities and those employed in the transport industries, primarily from acts of terrorism, and to retain public confidence in transport security, whilst not imposing requirements that impact disproportionately on the travelling public or on the effectiveness and efficiency of industry operations; and to co-ordinate the DfT's arrangements for responding to serious disruption of national life, actual or threatened, however caused."[1]

4. We examined the Secretary of State, and the Director and a deputy Director of TRANSEC, on 2 November. We are grateful to them, and to those who submitted written evidence against a short timescale, for their assistance. We acknowledge the assistance of Professor Paul Wilkinson, our Specialist Adviser.

5. Transport security is complex and, as we expected, the relevant issues could not be investigated thoroughly in a single evidence session. In consequence, we announced on 3 November a full inquiry into transport security, *Travelling without Fear*, with hearings in the New Year.[2]

6. **It was our initial intention to publish the evidence we received at our single hearing on transport security on 2 November without comment. But the terrorist threat is a current one, and we wish to highlight to the House, and the wider public, a number concerns arising from the hearing without delay. The scope of this report is not exhaustive however, and represents our initial impressions. We shall be looking further at these, and related matters, during our main inquiry in early 2006.**

---

1   Ev 1

2   Transport Select Committee, PN 13/2005-06, 3 November 2005

2 Matters for further investigation

Threat

7. The scale of the continuing threat to UK transport systems appears formidable. We have no reason to challenge the Secretary of State's sombre view of the present risk that 'it is one that we are going to be living under for the rest of our lives and probably our children's lives as well'.[3]

8. **We have no doubt that the threat to the travelling public in the UK from terrorist attacks remains grave. We shall examine the nature and threat that this presents to our transport networks thoroughly in the course of the forthcoming inquiry.**

Threat prediction

9. It is unlikely that any workable protective security system for transport networks can be completely effective at all times. The question is, whether and how the present protective security system can be improved. Its effectiveness is critically dependent upon the success of those responsible for providing information about the nature and timing of violent threats. As the Department notes 'Relevant and timely threat information must be a cornerstone of transport protective security regimes if they are to remain proportionate and flexible.'[4]

10. The destruction which terrorists inflicted upon travellers and the London Underground and bus network on 7 July represents a relative failure for the UK's protective security arrangements. The Director of TRANSEC said that 'what is never known, and it makes it very hard for us to assess the success of our job, what is never known publicly, and we do not know either, is what has not happened and what attacks have been prevented.'[5] This may be true, but is cold comfort to those affected directly by the events of 7 July.

11. **We shall seek to consider the process by which much protective security on our transport systems is based on 'relevant and timely threat information', and we shall examine what approaches the authorities may be considering to heighten practical protection for the travelling public.**

Co-operation within Government to meet attacks

12. The intelligence and security apparatus available to respond to the current threat of terrorism is necessarily complex. Unless lines of communication between the agencies are consistently excellent this complexity could slow urgent action in the event of an emergency. The example of the attack on the United States in 2001, which demonstrated

---

3   Q 26. 'Britain remains a target of the highest possible priority to al-Qaeda and its affiliates.' Sir Ian Blair, Metropolitan Police Commissioner, *Dimbleby Lecture 2005*, 16 November 2005, http://www.met.police.uk/

4   Ev 3

5   Q 26

substantial weaknesses in crisis management, communications and coordination on the part of those responsible for protective actions is chillingly before us :

> "We learned that the institutions charged with protecting our borders, civil aviation, and national security did not understand how grave this threat could be, and did not adjust their policies, plans, and practices to deter or defeat it. We learnt of fault lines within our government- between foreign and domestic intelligence, and between and within agencies. We learned of the pervasive problems of managing and sharing information across a large and unwieldy government that had been built in a different era to confront different dangers.'[6]

13. This must not happen in the UK. The Secretary of State said that there were lessons to learn after the events of 7 July, and that the Government was not complacent, but that a quick and co-ordinated response by agencies, transport operators, and Ministers to the July events had been made possible by training. Experience gained from previous incidents was also relevant.[7] He contrasted UK intra-agency cooperation where 'services work very closely together' with comparable US bodies which 'were fairly free standing and fairly independent of each other'.[8]

14. **We shall wish to test the positive view of the Secretary of State for Transport about coordination within Government to meet the terrorist threat, and the capacity of the emergency services to deal with a major terrorist incident on UK transport networks.**

Co-operation between Government and the transport industry

15. While TRANSEC is able to give directions to industry on the implementation of protective security measures,[9] good co-operation between the UK Government and the transport industry is the foundation of sound security for the travelling public. TRANSEC told us about the elaborate arrangements for ensuring co-ordination between the Government and transport industry, including a number of national security committees, sub-committees, and working groups, for each transport mode.[10] The Director of TRANSEC was positive about this relationship 'We share the problem with [industry], brief them on the threat, make sure that they understand the sort of threat that they might be under, and then we work with them to try to devise a measure that will meet that particular risk that we all share'[11].

Aviation sector

16. Evidence we received from the aviation sector reflected some tensions with the Government on security matters. British Airways told us that "there is over-regulation in

---

6   *The 9/11 Commission Report: Final Report of the National Commission On Terrorist Attacks Upon the United States,* New York, 2004, xvii

7   Q 32

8   Q 32

9   Q21

10   Ev 4

11   Q 21

the UK when compared with security regimes existing in both Europe and the US", which compromises the "competitive position of the United Kingdom's airlines and airports":[12]

> "In the UK there are more than 50 additional measures required by the Department for Transport and the Government to be implemented by UK airlines alone, over and above those stipulated within EU regulation".[13]

17. British Airways was unaware that any Regulatory Impact Assessment (RIA) had been undertaken "to demonstrate that the additional requirements are either proportionate or reasonable to address the assessed threat";[14] had an assessment been undertaken "its analysis and conclusions have not been shared with industry, nor was it consulted."[15] The Secretary of State thought that no RIA had been carried out. [16] We found this state of affairs surprising. **All security measures need to provide public reassurance while representing value for money. Our forthcoming inquiry will examine what action the Department is taking to achieve cost effectiveness in protective security for UK transport networks.**

18. Virgin Atlantic, too, expressed concerns about the absence of a review mechanism for security requirements. It also pointed to what it considered to be deficiencies in the efficiency of intra-governmental security co-ordination; a lack of cross border co-ordination with alleged "considerable duplication" between the Safety Regulation Group of the UK Civil Aviation Authority of the European Air Safety Authority (EASA); and the costs of recent anti terrorist security measures imposed by European governments on European airlines and airports which amounted to Euros 3 billion.[17] The company considered the present arrangements for a military response to bomb alerts on civil aircrafts to be inappropriate; and argued that denying airlines information about the UK 'country threat level' was 'unacceptable.'[18]

Other transport sectors

19. We had disquieting evidence from other parts of the transport industry. For example, the alleged poor state of some train radios on the London Underground which, it was claimed, could compromise safety in an emergency; and alleged inadequacies in the way procedures for identifying potentially dangerous packages in the Underground are being applied.[19]

20. The Road Haulage Association (RHA) expressed concerns that neither the costs nor staffing of a proposed Government scheme to allow police access to information to all

---

12   Ev 29

13   Ev 29

14   Ev 29

15   Ev 29

16   Qq 24, 25. *Transport Security & Contingencies Directorate (TRANSEC) Annual Report to Secretary of State for Transport,* April 2004-March 2005, received after the committee's hearing on 2 November, does make reference to a regulatory impact assessment in a separate area of TRANSEC work, in connection with the regulations for the security of transporting dangerous goods by road and rail which came into effect in July 2005, p 11

17   Ev 41

18   Ev 41

19   Ev 24

freight movements appear to have been assesed.[20] We were also told that an initiative to develop 'Truckwatch', a scheme "to ensure that a commercial vehicle and/or its cargo" may not be used as transport weapon, or to facilitate the delivery of a weapon, has stalled.[21]

21. The Road Haulage Association told us that co-ordination of transport security within Government must be improved;[22] and we heard about the high cost and evident unpopularity of the so-called "modal approach" to transport security in the industry from the Freight Transport Association.[23]

22. **We are not in a position at present to conclude whether the complaints we heard from the transport industry about the current protective security arrangements are justified, or to gauge their overall significance. It is obvious that effective security for the travelling public rests on sound co-operation between Government and the transport industry. While there is a developed structure of national security committees to ensure that this co-operation is effective, there is some evidence that improvements may be necessary.**

23. **The cost of transport security is never going to be popular with those who are required to pay. But it is essential that appropriate protective security measures are put in place for the UK transport network generally. These must be properly maintained and are upgraded regularly. There can be no compromise on this point. It is important that the Government reassures industry about the proportionate nature of the security measures required; and that industry adopts a realistic approach to meeting its obligations. We shall explore these matters further in our inquiry.**

TRANSPORT SECURITY AND CONTINGENCIES DIRECTORATE (TRANSEC)

Resources

24. To perform its tasks,[24] TRANSEC has a staff of 200 and a budget of £16.8 million,[25] 0.125 percent of the total public spending budget of the Department for Transport in 2003-04.[26]

25. The Director of TRANSEC said that she was 'satisfied with the numbers we have', and told us that her establishment is protected from staffing cuts.[27] She said that most comparable organisations abroad were 'envious' of TRANSEC's staffing levels.[28] The

---

20 Ev 27, 28

21 Ev 26

22 Ev 28

23 Ev 37

24 Paragraph 3

25 Ev 2

26 Department for Transport, *Annual Report 2005*, Cm 6527, June 2005, p 211. Measured against the 'estimated outturn' figures for 2004-05 in the Report, it represents 0.128 per cent. '[TRANSEC] currently comprises 200 posts. As at 1 November 2005 TRANSEC had eight staff working on a part time basis', HC Debate, 9 November 2005, col 522W. Q 58

27 Q 55

28 Q 57

Secretary of State told us that 'If there was a case to be made for employing more people, that would be something we would certainly look at.' But he appeared satisfied that TRANSEC had sufficient resources currently.[29] While these comments were broadly reassuring, it is vital that TRANSEC's resources fully match the current terrorist threat to UK transport. We have no details about how TRANSEC's budget is broken down currently. The Director of TRANSEC has undertaken to provide us with information on this, and we shall then make our own judgement about its resource levels.[30]

26. **Sufficient resources must be devoted to counter the terrorist threat to UK transport. We are aware that the budget of TRANSEC does not represent all Government spending on security. The transport industry's contribution also needs to be counted. The skilful deployment of TRANSEC's human and financial resources however is the key to focussing the UK's overall transport protective security regime.**

Operational matters

27. **There was no opportunity for us to examine in detail the wider operation of TRANSEC. For example, the approach adopted to enforcement, the value of international liaison, the reason for the prioritisation of security for 'closed' over 'open' transport systems, the application of technology to protective security, and a variety of security issues affecting the aviation, maritime, railway, bus, and underground sectors. Our forthcoming inquiry will include these aspects of TRANSEC's work.**

Reporting

28. TRANSEC is required to report annually to the Secretary of State for Transport, and a document is placed in the Library of the House of Commons.[31] The production of reports by TRANSEC originates in a commitment by the Government during the passage of the Aviation and Maritime Security Bill to report on the National Aviation Security Programme. Subsequent reports have extended beyond aviation.[32] **It is our firm view that TRANSEC should continue to report on its protective security activities, and that these reports should continue to be publicly available. But we have a number of concerns about the present arrangements.**

29. We were concerned at the absence of detail about corporate affairs in recent TRANSEC annual reports. The reports for 2003–04 and 2004–05 contain little detailed breakdown of expenditure, or information on human resources, which featured in earlier reports. The Director of TRANSEC said that 'perhaps too much detailed information had gone into the earlier reports and particularly now we wanted to get something that we put on our website which would be very accessible to the general public.'[33]

30. We did not find this argument particularly convincing. It is not obvious why omitting expenditure and human resources material from recent reports should enhance the

---

29   Q 54

30   Q 47

31   *TRANSEC Annual Report to Secretary of State for Transport*, April 2004—March 2005, p 3

32   Ibid, p 3

33   Q 47

accessibility of TRANSEC's website. **TRANSEC should explain any decision to adjust the level of information it provides publicly in its annual report. Such adjustments should be minimised to facilitate comparisons of its activity and performance year on year.**

31. TRANSEC annual reports contain no performance measures. We were assured that TRANSEC performance targets do exist,[34] and that internal monitoring procedures are in place.[35] TRANSEC's business plan is classified "because of all the material we bring together and it will tell you something about the vulnerabilities we perceive which we are working on."[36] **It should not be beyond the Department's capacity to devise performance measures for inclusion in TRANSEC's annual reports which avoid exposing classified information while at the same time providing a sound measure of public reassurance.**

32. Security is not included in the Department's Public Service Agreement (PSA). The Secretary of State pointed out that not all activities of the Department were reflected in the PSA.[37] **In the present circumstances consideration should be given by the Department to amending the PSA to include security. This would not only signal that work to protect the security of the travelling public was a priority for the Department, but would be a welcome statement of the Government's willingness to subject such work to Parliamentary and public scrutiny. We are pleased that the Secretary of State expressed himself willing to consider this**.[38]

33. **A more informative general approach to describing TRANSEC's 'front line' activities in the annual report could also be considered.** For example, a review of rail security was conducted in the wake of the terrorist attacks on the Madrid trains in 2004 and resulted in 'a package of 18 short, medium and long term measures to enhance rail counter-terrorist security'.[39] While there is some information about the review in the Department's separate submission to this committee,[40] the absence of detail about these measures in TRANSEC's annual report means that the reader is unable to judge their efficacy. Consequently, much of the point of the information is lost. Another example is the reference to the exercise code-named 'ATLANTIC BLUE' in which the report asserts TRANSEC participated successfully. But no further information is provided about it.[41]

34. TRANSEC's annual reports need to demonstrate convincingly how the Directorate's activities in the reporting year have contributed directly to enhancing the safety of the travelling public and the UK transport network. TRANSEC reports are made to the Secretary of State but are read by others. **We assume that the Secretary of State has access to separate information which enables him to make full sense of TRANSEC annual**

34   Q 51
35   Q 50
36   Q 50
37   Q 53
38   Q 53
39   TRANSEC *Annual Report 2004-05*, p 10
40   Ev 6
41   Ibid, p 14

reports' rather bare narratives. But for readers without such access, these reports require more contextual analysis and background to be fully adequate.

35. The rationale for TRANSEC continuing to have an annual report separate from the Department's *Annual Report* is not clear. The *Annual Report* already contains a short section on security,[42] and therefore covers some of the ground in the separate TRANSEC document. **The Department may wish to consider whether bringing TRANSEC's reports within the Department's *Annual Report* would avoid duplication. The *Annual Report* has a wider circulation than TRANSEC's document, and making this change could represent some increase in transparency for UK transport protective security activities.**

36. We were also concerned about the length of time between the close of the latest reporting period, March 2005, and the report being received in the Library of the House of Commons, November 2005, almost eight months. While this is an improvement on the publication of the report for April 2003 to March 2004 which, according to the Department's website, was published on 5 April 2005, it remains too long.[43] The latest annual report extends to sixteen pages, and a report of this length should not take the best part of a year to produce.

37. **Annual reports as spartan as those of TRANSEC represent a missed opportunity to refresh outreach with the travelling public about the crucial importance of security on the UK transport network. TRANSEC needs urgently to improve the presentation and content of these. If future reports are to be useful and credible, a rigorous effort must be made to distinguish between material which is genuinely sensitive from that which can be disclosed. The reports should contain performance measures, and consideration should be given to including security within the Department's Public Service Agreement. Reports should be made within a reasonable time of the end of the reporting period.**

Public confidence in TRANSEC

38. The public must have confidence in those who regulate the security of our transport networks. TRANSEC aims 'to retain public confidence in transport security'.[44] Without this confidence, the full co-operation of the public is unlikely to be forthcoming when security measures on UK transport networks are implemented. While it is self-evidently in every traveller's interest to exercise vigilance and to report suspicious circumstances to the authorities, many security measures slow travellers' journeys and, for that reason, are in themselves unwelcome. In addition, the implementation of new security measures is an additional responsibility for transport operators.

39. **High awareness amongst the travelling public is one of the greatest potential assets in the common defence against terrorist outrages on the UK transport network. In the course of our forthcoming inquiry we shall examine what the Government, TRANSEC**

---

42   Department for Transport, *Annual Report 2005*, pages 193-195

43   Department for Transport website at
     www.dft.uk/stellent/groups/dft_transsec/documents/page/dft_transec_037131.hcsp

44   Ev 1

and industry are doing to enlist the support of the public systematically in the co-operative effort to counter the present terrorist danger; and what training is offered to transport staff to ensure that those in the 'front line' of transport networks are able to cope with any future terrorist incidents.

Secretary of State for Transport's announcement on 2 November 2005

40. **In the course of his evidence to us on 2 November, the Secretary of State announced that new security equipment was to be tested on the railway and underground networks in London next year. We warmly welcome this evidence of activity on the part of the authorities to explore ways of making travel safer.[45] We expect the Department for Transport to publish the results of the trials, and to explain the basis of future decisions on any permanent deployment of such equipment on the networks.**

Media

41. Sensationalist media reporting of terrorism stimulates fear without adding value to the debate on ways to prevent outrages. Comprehensive, balanced and accurate media reporting about terrorist organisations, threats to transport networks, and the Government's response, is an important aspect of the effort to combat what is a largely hidden threat. Such reporting can expose the irresponsibility and inhumanity of terrorism.[46]

42. **We were surprised to see on TRANSEC's part of the Department's website the statement that 'we do not think it is helpful for the media to highlight alleged weaknesses that may tempt those with questionable motives to seek to exploit them.' While encouragement must not be given to those seeking to disrupt our transport systems, we think it may be simplistic to urge the media to desist from reporting flaws in protective security when these are uncovered. We expect the relevant authorities to deal swiftly and effectively with security weaknesses, and with those who would exploit them. We shall be interested to pursue the effect of media reporting of transport security incidents in our inquiry.**

3 Conclusion

43. **We hope that no city will experience events similar to those which took place in London on 7 July 2005. These events demonstrated the paralysing disruption terrorist attacks can cause to the transport infrastructure of a major city. The threat of further attacks remains very high. The means at the disposal of the UK Government to counter terrorist threats to the travelling public must be deployed effectively and efficiently.**

44. **Public vigilance is one of the greatest assets in countering the dangers of terrorism on the transport network. The Department for Transport's policy of protective security**

---

45   'New Security Equipment To be Tested On Rail and Underground Network', Department for Transport, News Release 2005/0110, 2 November 2005

46   Paul Wilkinson, *Terrorism versus Democracy*, London, 2000, p 183

needs to be vigorously proactive in order to engage each member of the travelling public as a partner in helping, where possible, to prevent future terrorist attacks on the transport network. Imaginative policies and inspiring leadership are called for, and TRANSEC is positioned to help provide this.

45. **The Secretary of State for Transport and TRANSEC were broadly reassuring when we questioned them on 2 November. The trials of new screening equipment in railway and London Underground stations announced then, and planned for implementation early next year, are welcome. We hope that these are the first of many protective security innovations designed to place those who would kill without compunction firmly on the defensive.**

46. **We have no doubt that the staff of TRANSEC, and the Department generally, are dedicated to reducing the threat of terrorism faced by the travelling public. But the concerns set out in this preliminary report remain. We intend to examine these, and the security of UK transport generally, further in our forthcoming inquiry before coming to final conclusions.**

Conclusions and recommendations

1. It was our initial intention to publish the evidence we received at our single hearing on transport security on 2 November without comment. But the terrorist threat is a current one, and we wish to highlight to the House, and the wider public, a number concerns arising from the hearing without delay. The scope of this report is not exhaustive however, and represents our initial impressions. We shall be looking further at these, and related matters, during our main inquiry in early 2006. (Paragraph 6)

2. We have no doubt that the threat to the travelling public in the UK from terrorist attacks remains grave. We shall examine the nature and threat that this presents to our transport networks thoroughly in the course of the forthcoming inquiry. (Paragraph 8)

3. We shall seek to consider the process by which much protective security on our transport systems is based on 'relevant and timely threat information', and we shall examine what approaches the authorities may be considering to heighten practical protection for the travelling public. (Paragraph 11)

4. We shall wish to test the positive view of the Secretary of State for Transport about coordination within Government to meet the terrorist threat, and the capacity of the emergency services to deal with a major terrorist incident on UK transport networks. (Paragraph 14)

5. All security measures need to provide public reassurance while representing value for money. Our forthcoming inquiry will examine what action the Department is taking to achieve cost effectiveness in protective security for UK transport networks. (Paragraph 17)

6. We are not in a position at present to conclude whether the complaints we heard from the transport industry about the current protective security arrangements are justified, or to gauge their overall significance. It is obvious that effective security for the travelling public rests on sound co-operation between Government and the transport industry. While there is a developed structure of national security committees to ensure that this co-operation is effective, there is some evidence that improvements may be necessary. (Paragraph 22)

7. The cost of transport security is never going to be popular with those who are required to pay. But it is essential that appropriate protective security measures are put in place for the UK transport network generally. These must be properly maintained and are upgraded regularly. There can be no compromise on this point. It is important that the Government reassures industry about the proportionate nature of the security measures required; and that industry adopts a realistic approach to meeting its obligations. We shall explore these matters further in our inquiry. (Paragraph 23)

8. Sufficient resources must be devoted to counter the terrorist threat to UK transport. We are aware that the budget of TRANSEC does not represent all Government spending on security. The transport industry's contribution also needs to be counted. The skilful deployment of TRANSEC's human and financial resources however is the key to focussing the UK's overall transport protective security regime. (Paragraph 26)

9. There was no opportunity for us to examine in detail the wider operation of TRANSEC. For example, the approach adopted to enforcement, the value of international liaison, the reason for the prioritisation of security for 'closed' over 'open' transport systems, the application of technology to protective security, and a variety of security issues affecting the aviation, maritime, railway, bus, and underground sectors. Our forthcoming inquiry will include these aspects of TRANSEC's work. (Paragraph 27)

10. It is our firm view that TRANSEC should continue to report on its protective security activities, and that these reports should continue to be publicly available. But we have a number of concerns about the present arrangements. (Paragraph 28)

11. TRANSEC should explain any decision to adjust the level of information it provides publicly in its annual report. Such adjustments should be minimised to facilitate comparisons of its activity and performance year on year. (Paragraph 30)

12. It should not be beyond the Department's capacity to devise performance measures for inclusion in TRANSEC's annual reports which avoid exposing classified information while at the same time providing a sound measure of public reassurance. (Paragraph 31)

13. In the present circumstances consideration should be given by the Department to amending the PSA to include security. This would not only signal that work to protect the security of the travelling public was a priority for the Department, but would be a welcome statement of the Government's willingness to subject such work

to Parliamentary and public scrutiny. We are pleased that the Secretary of State expressed himself willing to consider this (Paragraph 32)

14. A more informative general approach to describing TRANSEC's 'front line' activities in the annual report could also be considered. (Paragraph 33)

15. We assume that the Secretary of State has access to separate information which enables him to make full sense of TRANSEC annual reports' rather bare narratives. But for readers without such access, these reports require more contextual analysis and background to be fully adequate. (Paragraph 34)

16. The Department may wish to consider whether bringing TRANSEC's reports within the Department's Annual Report would avoid duplication. The Annual Report has a wider circulation than TRANSEC's document, and making this change could represent some increase in transparency for UK transport protective security activities. (Paragraph 35)

17. Annual reports as spartan as those of TRANSEC represent a missed opportunity to refresh outreach with the travelling public about the crucial importance of security on the UK transport network. TRANSEC needs urgently to improve the presentation and content of these. If future reports are to be useful and credible, a rigorous effort must be made to distinguish between material which is genuinely sensitive from that which can be disclosed. The reports should contain performance measures, and consideration should be given to including security within the Department's Public Service Agreement. Reports should be made within a reasonable time of the end of the reporting period. (Paragraph 37)

18. High awareness amongst the travelling public is one of the greatest potential assets in the common defence against terrorist outrages on the UK transport network. In the course of our forthcoming inquiry we shall examine what the Government, TRANSEC and industry are doing to enlist the support of the public systematically in the co-operative effort to counter the present terrorist danger; and what training is offered to transport staff to ensure that those in the 'front line' of transport networks are able to cope with any future terrorist incidents. (Paragraph 39)

19. In the course of his evidence to us on 2 November, the Secretary of State announced that new security equipment was to be tested on the railway and underground networks in London next year. We warmly welcome this evidence of activity on the part of the authorities to explore ways of making travel safer. We expect the Department for Transport to publish the results of the trials, and to explain the basis of future decisions on any permanent deployment of such equipment on the networks. (Paragraph 40)

20. We were surprised to see on TRANSEC's part of the Department's website the statement that 'we do not think it is helpful for the media to highlight alleged weaknesses that may tempt those with questionable motives to seek to exploit them.' While encouragement must not be given to those seeking to disrupt our transport systems, we think it may be simplistic to urge the media to desist from reporting flaws in protective security when these are uncovered. We expect the relevant authorities to deal swiftly and effectively with security weaknesses, and with those

who would exploit them. We shall be interested to pursue the effect of media reporting of transport security incidents in our inquiry. (Paragraph 42)

21. We hope that no city will experience events similar to those which took place in London on 7 July 2005. These events demonstrated the paralysing disruption terrorist attacks can cause to the transport infrastructure of a major city. The threat of further attacks remains very high. The means at the disposal of the UK Government to counter terrorist threats to the travelling public must be deployed effectively and efficiently. (Paragraph 43)

22. Public vigilance is one of the greatest assets in countering the dangers of terrorism on the transport network. The Department for Transport's policy of protective security needs to be vigorously proactive in order to engage each member of the travelling public as a partner in helping, where possible, to prevent future terrorist attacks on the transport network. Imaginative policies and inspiring leadership are called for, and TRANSEC is positioned to help provide this. (Paragraph 44)

23. The Secretary of State for Transport and TRANSEC were broadly reassuring when we questioned them on 2 November. The trials of new screening equipment in railway and London Underground stations announced then, and planned for implementation early next year, are welcome. We hope that these are the first of many protective security innovations designed to place those who would kill without compunction firmly on the defensive. (Paragraph 45)

24. We have no doubt that the staff of TRANSEC, and the Department generally, are dedicated to reducing the threat of terrorism faced by the travelling public. But the concerns set out in this preliminary report remain. We intend to examine these, and the security of UK transport generally, further in our forthcoming inquiry before coming to final conclusions. (Paragraph 46)

Formal minutes

Wednesday 23 November 2005

Members present:

Mrs Gwyneth Dunwoody , in the Chair

Mr David Clelland   Mr Eric Martlew
Clive Efford   Mr John Leech
Mrs Louise Ellman   Mr Lee Scott
Mr Robert Goodwill

The Committee deliberated.

Draft Report (*UK Transport Security – preliminary report*), proposed by the Chairman, brought up and read.

Ordered, That the draft Report be read a second time, paragraph by paragraph.

Paragraphs 1 to 46 read and agreed to.

Ordered, That the Appendices to the Minutes of Evidence taken before the Committee be reported to the House.

Ordered, That the provisions of Standing Order No. 134 (Select committee (reports)) be applied to the Report.

Ordered, That the Chairman do make the Report to the House.

[Adjourned till Wednesday 30 November at half past two o'clock.

Witnesses

List of written evidence

Reports from the Transport Committee since 2005

Oral evidence

Taken before the Transport Committee

on Wednesday 2 November 2005

Members present:

Mrs Gwyneth Dunwoody, in the Chair

Mr David Clelland	Mr John Leech
Mr Jeffrey Donaldson	Mr Eric Martlew
Clive Efford	Mr Lee Scott
Mrs Louise Ellman	Graham Stringer
Mr Robert Goodwill	

Memorandum submitted by the Department for Transport

INTRODUCTION

1. The purpose of this memorandum is to provide the Transport Select Committee with an account of the Department's responsibilities for transport security (land, aviation and maritime), its role in the aftermath to the London bomb attacks of July 2005 and its role as the coordinator for contingency planning within the Department. The memorandum includes information on:

— the overall aims and objectives of the Transport Security and Contingencies Directorate (TRANSEC) of the Department for Transport (DfT), and key processes of transport security;

— rail security and the attacks of 7 and 21 July;

— history, staffing, resources, oversight and business planning;

— the role of TRANSEC within Government;

— programme development and relationship with industry;

— breakdown of modal transport security regimes—land, aviation and maritime, and the broad contingency arrangements in place;

— transport security from an international and EU perspective;

— financing transport security;

— the role of technology; and

— recruitment, vetting and training.

AIMS AND OBJECTIVES

Aim

2. Transport security is regulated by TRANSEC which is responsible for developing and enforcing the security standards required of transport operators. Its aim is:

"to protect the travelling public, transport facilities and those employed in the transport industries, primarily from acts of terrorism, and to retain public confidence in transport security, whilst not imposing requirements that impact disproportionately on the travelling public or on the effectiveness and efficiency of industry operations; and to co-ordinate the DfT's arrangements for responding to serious disruption of national life, actual or threatened, however caused."

Objective

3. A key objective of transport security is to ensure that effective and proportionate security regimes are maintained across all of the regulated transport security modes, addressing threats to and vulnerabilities in domestic and overseas operations, and taking account of new and emerging threats, including to transport "soft targets".

4. Furthermore, the transport security regimes are designed whenever possible to detect an act of terrorism before it is committed and prevent it happening. Some measures may deter the would-be perpetrator. Others have value in terms of public reassurance.

Key Processes of Transport Security

5. A key component underpinning the security regimes is to have, both at home and overseas, proportionate, pragmatic and sustainable security that does not place an undue burden on UK industry and does not discourage the travelling public from travelling. A "layered approach" to security acknowledges that no single security measure is either fool-proof, or capable of mitigating every type of threat. The aim, therefore, is to reduce the risk rather than seek to eliminate it entirely.

6. Each regime combines "front line" security measures (eg screening, searching, physical barriers, patrolling) designed to prevent, detect or deter a terrorist attack, with secondary measures (eg background checks, security vetting, training) focusing on the quality and integrity of staff.

7. Mature and well developed security regimes have been in place since the early 1990s for the aviation, maritime and Channel Tunnel sectors. Since 2000, the national rail, London Underground and the Docklands Light Railway networks have been regulated, with the Glasgow Subway to follow from November 2005. The regulatory framework was extended to the security of dangerous goods in transport in July 2005.

8. The regulatory regimes are implemented through the serving of legal directions on the industry by TRANSEC, and supported by detailed written programmes which provide advice on delivery. A comprehensive inspection and enforcement process—led principally by TRANSEC inspectors—underpins the regimes.

9. Detailed descriptions of the work and priorities of TRANSEC's land transport, aviation and maritime security regimes and its contingencies activities are attached at *Annexes A, B, C and D respectively*. The Land Transport Annex provides a brief account of TRANSEC's role in the aftermath to the London bombings of July 2005.

History, Staffing, Resources, Oversight and Business Planning

History

10. TRANSEC was established in 1991 as a result of the Lockerbie disaster building on what had been the Aviation Security Division in DfT. Its responsibilities were extended to cover maritime security in the early 1990s and then further extended to cover the Channel Tunnel, national railways, London Underground and the security of dangerous goods in transport over the following decade. The UK was the first country in the world to establish a comprehensive cross-modal security authority in government—a pattern now being adopted elsewhere, notably in the USA and Australia.

Staffing

11. Between December 1988 (the time of the Lockerbie disaster) and 1994, TRANSEC expanded from 15 to about 125 posts. A subsequent efficiency round led to a reduction in posts to 81 by 2001.

12. TRANSEC's role increased significantly following the 11 September 2001 and the Madrid 2004 attacks and increased international security activity over this period. The DfT Board agreed the resulting growth in TRANSEC to meet the major new obligations, challenges and expectations, and since 2002 TRANSEC's headcount has increased to 200 posts with an overall annual budget of £16.8 million.

Oversight and business planning

13. TRANSEC's work is planned in line with the DfT's business planning framework. TRANSEC contributes to the Departmental Business Plan and has its own detailed annual business plan which is security classified. In addition, its work is an integral part of the Government's wider counter-terrorism programme.

14. Oversight of TRANSEC's work is undertaken through its reporting to the Secretary of State and the DfT Board. On a Directorate basis its business plan, including consideration of risks to delivery is managed by the Director[1] through her divisional managers and internal Programme Management Group.

15. The Secretary of State places TRANSEC's annual report in the House of Commons' Library.

TRANSEC's Position within DfT and within Government

Position within DfT

16. TRANSEC sits within the DfT, reporting to the Secretary of State but it operates independently from the transport policy Directorates. Thus positioned, it can be aware of, but not inappropriately influenced by the Department's industry "sponsorship" considerations.

---

[1] Current TRANSEC Director is Niki Tompkinson.

Position within Government

17. The Government's long-term counter-terrorism strategy—CONTEST—is overseen by the Cabinet Office. Its aim is to reduce the risk from international terrorism so that people can go about their business freely and with confidence. In strategic terms, reducing the risk is undertaken across four broad mission areas (also known as the four "P"s):

— *Prevent*—terrorism by tackling its underlying causes;

— *Pursue*—terrorists and those that sponsor them;

— *Protect*—the public and UK interests through better protective security; and

— *Prepare*—for the consequences and to improve our resilience to cope with attacks and other major disruptive challenges.

18. Transport security and contingencies have been and remain key components in the "Protect" and "Prepare" pillars of that strategy.

19. Transport security has recently been established as a separate workstream within the CONTEST "Protect" structure which should provide a more robust and effective framework for closer working with key Government stakeholders, notably the police (primarily the Metropolitan Police Service (MPS) and the British Transport Police (BTP)) and the Security Service (who advises the transport industries on physical security and electronic attack).

PROGRAMME DEVELOPMENT AND RELATIONSHIP WITH INDUSTRIES

Relationships with industry

20. Responsibility and accountability for the design and delivery of security programmes are shared between the transport operators who own and manage the transport systems, and the Government. Government activity is divided between:

— the DfT, which directs and advises the industry (including on the basis of threat assessments from the Joint Terrorism Analysis Centre (JTAC));

— the security agencies—the National Security Advice Centre (NSAC) and the National Infrastructure Security Coordination Centre (NISCC), which offer the industry expert advice on electronic security; and

— the Police, who have a wider responsibility to prevent and detect crimes and to respond to major incidents and emergencies.

21. In addition, TRANSEC and the Foreign & Commonwealth Office (FCO) advise on the protection of UK transport assets and citizens overseas.

22. The Police's counter-crime and counter-terrorist programmes make an important contribution to transport security in deterring acts of unlawful interference, in providing public reassurance and an immediate response to any security incident. The BTP and the MPS have produced detailed complementary strategies designed to provide an over-arching approach for co-ordinating the Police response towards countering a heightened threat from terrorism on the "open" transport networks.

The threat

23. There is a history of transport not only being attacked but being used as the means of attack. Protective security regimes need to minimise both of these risks. They address the threat from both conventional and unconventional terrorist attacks, and recognise that there are many soft targets (particularly on the "open" land transport networks) as well as the traditional harder targets (eg aircraft), and therefore a wide range of possible attack scenarios.

24. Relevant and timely threat information must be a cornerstone of transport protective security regimes if they are to remain proportionate and flexible. However, it is also important to take vulnerability and consequences into account when making decisions about levels of security.

25. To inform the more detailed analysis of the effectiveness of the current regimes, JTAC produces up-to-date threat assessments, which include an identification of the most likely terrorist *modus operandi* that could be used against the transport network. An important aspect of TRANSEC's work is to inform the relevant UK industry of any changes in the threat levels and the required response measures. This is done by a secure means of communication, available on a 24/7 basis.

Baselines and enhanced measures—risk assessment process

26. The regulated programmes all have "baselines" of measures that remain in place regardless of the threat. The baselines are enhanced in response to increases in the threat in order to maintain the risk at an acceptable level. Baselines are set in accordance with prevailing threat levels, international requirements, the history of attacks, the inherent vulnerability of the mode of transport, whether it is an "open" or "closed" system and the potential consequences of a successful attack. Account also has to be taken of operational realities: security measures that bring transport to a standstill would deliver the terrorists' objective for them.

Stepped approach to enforcement

27. As well as being the security regulator, TRANSEC seeks to build positive relationships with the transport industries to encourage their compliance. It works closely with transport operators to develop security measures and practices that are effective, sustainable and responsive to the changing nature of security threats. TRANSEC pursues security improvements that are responsive to commercial realities, and works with industry to ensure robust security while meeting the increasing demand for travel.

28. The compliance model used by TRANSEC is applied consistently to all transport modes. It follows a stepped approach with the primary emphasis on co-operation, advice, dialogue and self-rectification, followed up through enforcement and, in the worst or persistent cases, prosecution. Experience to date has shown that prosecution has not been necessary as industry has been willing to implement remedial action when breaches, or potential breaches, of security have been highlighted by the Department.

National committee structures and communications with industry

29. TRANSEC operates on a number of levels:
— TRANSEC liaises with senior industry officials and nominated security contacts on a wide range of security issues including the dissemination of relevant threat assessments;
— Protective security regimes are overseen by national security committees for each transport mode. These comprise all key industry stakeholders and the Police, and whose bi-annual meetings are chaired at senior official and ministerial level. Their remit is to maintain an overview of the standard of security and to discuss any concerns arising; and
— Below the national committees, various sub-committees and working groups ensure that Government and industry continue to work together effectively.

Financing Security

30. It has been the policy of successive Governments that the cost of transport security should be borne by those that use the transport systems rather than by the general taxpayer. Thus, the costs of providing security measures on the ground fall to each transport industry, and are passed on to the end user, the passenger, as appropriate.

31. Industry is not required to meet the costs of security regulation or compliance monitoring. Furthermore, Government departments and the Police pick up the costs of the funding of research, development and evaluation of technologies and other systems to support the industries' provision of security. This includes the provision of advice, some contribution to training courses, training aids, and the administration of counter-terrorist checks for relevant staff in the industries. The Government also funds TRANSEC's considerable international effort, designed to enhance the security of the industries' overseas operations.

International and EU Activity

32. The international community has responded to the changed security environment by expanding existing, and developing, new international protective security regimes, a process which TRANSEC has actively supported. This includes:
— the development of international aviation security at the EU level and through the International Civil Aviation Organisation (ICAO) and the European Civil Aviation Conference (ECAC);
— the greater prominence given to maritime security by the International Maritime Organisation's (IMO) new regime;
— international concerns about the secure transport of dangerous goods which have been reflected in recently adopted United Nations and EU security requirements; and
— TRANSEC's long-established working relations with French counterparts on security in the Channel Tunnel.

33. Work in the EU is the highest priority from an international perspective. Over the years, the European Commission has introduced regulations governing key aspects of maritime and aviation security. It also introduced in 2005 regulations governing the transport security of dangerous goods. On supply chain (freight) security TRANSEC expects to see a Communication from the Commission in late 2005.

34. TRANSEC enjoys significant influence and respect internationally as a result of its expertise, experience and high standards of transport security in the UK. This is demonstrated by the many international delegations it receives on a regular basis and the many requests for TRANSEC's input into international exchanges.

ROLE OF TECHNOLOGY

35. Technology is at the heart of many key security measures. Developments in technology can bring improvements in security and/or reduce costs eg through more reliable detection of terrorist weaponry, or by reducing the amount of direct human intervention. Technology can also permit the implementation of measures that cannot be carried out manually.

36. TRANSEC sponsors a programme of research, development and technical evaluation (R&D&E). The programme has four key objectives with the common aim of improving transport security:

— fund research and development of promising ideas to the point at which the idea is proven to have sufficient potential that commercial developers will take it on;

— evaluate new equipment or technology-based security processes to establish their effectiveness and suitability for transport security applications;

— enhance the effectiveness of security technologies by collaboration with manufacturers to refine their designs and by research and development focused on improving the way security personnel use technology; and

— inform the development of the modal security programmes by conducting research to identify and characterise security vulnerabilities, to assess the likely impact of attack scenarios and to evaluate options to prevent or mitigate an attack.

37. *Annex E* provides a brief summary of some of the key outcomes from the TRANSEC R&D&E Programme during the financial year 2004–05.

RECRUITMENT, VETTING AND TRAINING

Recruitment and vetting

38. Varying degrees of recruitment and vetting practices—regulatory and advisory—operate within the transport industries, depending largely on the "closed" or "open" nature of the transport system, the sensitivity of the security posts and functions, the maturity of the security framework and the needs of the industry.

39. The most established regime exists in the aviation industry with vetting for airport staff with security duties beginning in March 1997. Since 2003, certain security duties in the maritime and Channel Tunnel industries have carried a requirement to undergo vetting in the form of employer recruitment and counter-terrorist checks. There are no mandatory requirements on vetting of general rail staff with security duties, although guidance is offered.

Training

40. Other than the mandatory security training in the aviation industry, training in the other transport modes is on an advisory basis, though plans are in place to regulate here too. Where appropriate, TRANSEC specifies the content of the courses, formally approves providers and monitors the quality of the training. It also contributes to courses by providing lecturers and administrative support. The Security Service plays an important role in assisting with this work.

CONCLUSION

41. Transport security has well developed and mature programmes of regulation and guidance in place since the early 1990s, augmented by the strong working relationships that have been forged between the Government and industry, and between the various Government stakeholders. Having already implemented measures for the largely "closed" transport systems which TRANSEC deems to be pragmatic, proportionate and cost-effective, the challenge now lies in developing the options for addressing "open" systems and new modes of attack.

42. The focus of TRANSEC's work programme remains to ensure that its proportionate security regimes are maintained across all of the regulated transport security modes, addressing risks and vulnerabilities in domestic and overseas operations, and taking account of new and emerging threats, including to transport "soft targets".

Department for Transport

20 October 2005

Annex A

Land Transport Security and the London July Attacks

1. Security regulation was introduced in the Channel Tunnel network in 1994, the heavy rail network in February 2000, the light rail network (London Underground) in October 2003 and the Docklands Light Railway in September 2005. From November 2005, the Glasgow Subway will be formally regulated. From July 2005, the security of dangerous goods in transport was also brought under formal regulation.

2. Industry is responsible for the implementation of the regulated security measures. DfT inspectors monitor and enforce compliance against the security standards.

3. The hierarchy of measures are devised in response to the mode-specific threat levels identified by the intelligence services. An important aspect of TRANSEC's work is to inform the relevant UK industry of any changes in the threat levels and the required response measures. This is done by a secure means of communication, available 24/7.

Pre-Madrid security regime

4. Rail security in Great Britain has strong foundations in place which have been developed over time to deter the Irish terrorist threat. Its focus has been on bombs left in stations and, to some extent, on trains, and to make it as hard as possible to leave unattended items. Many of the security measures in place (left luggage screening, station searches, restrictions on litter bins and BTP-developed rail staff procedures to evaluate the risk associated with the discovery of an unattended item) were specifically developed to deal with that threat.

Post-Madrid review of rail and underground security

5. Following the Madrid rail attacks in March 2004, TRANSEC undertook a comprehensive review to examine rail security measures already in place nationally and investigate new ways of improving those measures. It was undertaken in conjunction with the BTP, industry and other Government departments.

6. The outcomes of the review, endorsed by Government in late 2004, identified a package of short, medium and long-term measures to enhance rail counter-terrorist security and for industry to deliver. These centred on: new regulatory measures; new and improved guidance; better working arrangements with the BTP and industry; and further studies into long-term transport security issues.

7. A key feature of the review was to ensure that the measures were proportionate, pragmatic, sustainable and did not place an undue burden on industry. The measures were designed for the prevailing threat at the time and to be introduced without requiring a significant shift in the "open" nature of the rail system. Furthermore, the measures not only continued to address the threat from bombs deposited on stations but also extended the focus to trains.

8. Running in parallel with the Madrid review, the BTP produced in December 2004 its National Strategic Framework which was designed to provide an over-arching approach for co-ordinating the police response towards countering a heightened threat from terrorism upon the rail network. It describes how it could provide a national capability that takes into account alterations to the threat level.

Rail security post-7 July

9. The 7 July attacks against the London Underground were the first suicide attacks in the UK. On that day, the mandatory security requirements were raised to their highest level across the rail and underground networks resulting in the tightening of the existing measures. Prompted in part by TRANSEC, industry also introduced measures over and above their regulatory requirements, previously agreed with TRANSEC.

10. A rail industry working group has been convened to keep under review existing security policies and consider any further areas for action following the London attacks. This will ensure greater and more prompt focus is given to the full range of rail security issues.

11. TRANSEC is collaborating with NSAC to support its research and development activities in a number of areas that are of relevance to transport security. These include:

— evaluation and development of "Intelligent Vision Systems"—CCTV;

— investigation into blast effects and blast mitigation strategies, with a particular emphasis on blast on tube trains; and

— behavioural sciences—including techniques for identifying suspicious behaviour.

Bus and coach security

12. TRANSEC will issue to all bus and coach companies in the United Kingdom in November 2005 protective security advice and guidance. This will be based in part on the regimes TRANSEC has in place for elements of the rail industry.

Annex B

AVIATION SECURITY

1. Security regulation was introduced into the aviation sector through the Aviation Security Act 1982. TRANSEC is responsible for regulating and monitoring compliance with aviation security standards in the UK. It also works to protect UK airline operations overseas, including by pressing for higher standards and better implementation internationally.

2. Under the 1982 Act, TRANSEC issues Directions to airlines, airports and others and requires these "Directed Parties" to carry out the measures specified—such as the screening of passengers and their bags. Directions are written in broad terms, leaving industry managers to identify the optimum means of implementing the requirements. They specify the minimum standard required though industry can apply additional measures should it choose to do so. The Directions, together with the recommended practices which indicate how standards may be best applied, make up the National Aviation Security Programme (NASP).

3. Measures are primarily ground-based. The airport Restricted Zone (RZ) is a *"cordon sanitaire"* in which all passengers, staff, baggage and cargo are subject to screening. As in other modes, security is layered; it is a combination of measures rather than a single line of defence.

4. Ensuring that measures are implemented effectively is crucial. TRANSEC inspectors assess the delivery of security on the ground to ensure that the required standards are being met. TRANSEC maintains a constructive dialogue with industry at all levels and encourages them to take ownership and responsibility for ensuring standards are being met. TRANSEC seeks rectification where appropriate and takes enforcement action where necessary.

5. The delivery of effective aviation security requires co-ordinated working between stakeholders, including government, industry and the police and other control authorities. Sir John Wheeler's 2002 report on aviation security, commissioned by Government, endorsed TRANSEC's role in this relationship. It also concluded that multi-agency analytical work on the threat of serious and organised crime to airport security was required in order to develop a more holistic approach. This recommendation led to the establishment of the Multi-Agency Threat and Risk Assessment (MATRA) process at UK airports.

6. Under MATRA, those with a stake in the security of the airport work together to agree a risk register and identify further actions required to mitigate risks to an acceptable level, which ultimately leads to an airport security plan. This voluntary process is supported by a joint DfT/Home Office secretariat, which promotes best practice and monitors progress. MATRA has created greater mutual familiarity between stakeholders for each other's responsibilities, ways of working, issues and concerns.

7. Since 9/11, the overall pace and scope of international aviation security work has increased dramatically and a large number of initiatives have been taken forward. As a comprehensive regime already existed in the UK, relatively little change to UK practice was required. Some of our international partners faced a greater challenge in raising their levels of protective security. There has been a greater impetus in a number of international organisations to develop new aviation security standards and initiatives. This has called for even greater engagement by TRANSEC internationally, both multilaterally in the EU, ICAO, ECAC and G8, and through an intensified programme of overseas assessments and other bilateral work.

8. Work in the EU is the highest priority from an international perspective as EC Regulations are directly applicable in UK law, and bear on key neighbouring States with major traffic flows to the UK. The UK engages closely in the work of the EC Regulatory Committee which develops the regulatory standards and implementing procedures for aviation security in the EU, and is contributing actively to the present recasting of the baseline EU regulation, in light of two years' experience of its application.

9. The UK also plays a very active role in ICAO and a high priority is to try to raise the security baseline and to press for ICAO standards which are more directly relevant to the current threat scenario. TRANSEC also makes best use of opportunities in international fora to raise awareness of the seriousness and global nature of the threat to aviation.

10. TRANSEC carries out a major programme of overseas assessments, in co-operation with Host State authorities. This programme concentrates primarily on UK airline operations to encourage standards which will enable UK airlines to operate securely. In addition, an intensified programme of visits to the UK by aviation security specialists from foreign governments allows TRANSEC to promote and demonstrate UK aviation security philosophy and best practice to those best placed to influence standards overseas.

11. TRANSEC has developed a small network of Regional Aviation Security Liaison Officers (RASLOs) based overseas to work collaboratively with international partners and UK airlines in key regions around the world, providing technical and specialist support, training and guidance. TRANSEC has been actively involved in training activities internationally for many years. This has particular benefits at locations where UK airlines operate but also serves to improve the security environment for other airline operations to the UK.

Annex C

Maritime Security

1. Security regulation was first introduced into the maritime sector through the Aviation & Maritime Security Act 1990. TRANSEC is responsible for regulating maritime security and monitoring compliance in the UK. It also works to protect UK maritime operations overseas, including by pressing for higher standards and better implementation internationally.

2. TRANSEC is given operational support by the Maritime and Coastguard Agency (MCA) in ensuring that UK registered cargo vessels are compliant with the requirements of the International Ship and Port Security (ISPS) Code. UK passenger vessels, ferry services and all of the UK's port facilities serving ships engaged on international voyages fall within the work of TRANSEC directly. It also maintains general oversight of the maritime security arrangements for the Overseas Territories and Crown Dependencies.

3. An important aspect of TRANSEC's work is to inform the UK shipping and port industries of changes in the security levels in response to threat information that is received by TRANSEC from the intelligence services. This is done by a secure means of communication.

4. The implementation of the ISPS Code in July 2004 represented a major change in the way maritime security was regulated. Developed by the IMO and given effect by European regulation, it has been embraced by the shipping and ports industries where levels of compliance were satisfactory.

5. TRANSEC worked with industry to introduce security measures that were proportionate and sustainable. There is now a programme of compliance to ensure that the security plans agreed and approved by TRANSEC and the MCA are in place. TRANSEC works with the EC and Member States to ensure that compliance with the requirements is being achieved internationally. Where necessary, it engages in capacity building initiatives in partnership with the EC, G8 States and the IMO.

6. The maritime security programme includes engaging with other Government Departments to provide assurance that an effective response to maritime threats and incidents can be mounted. Specifically, TRANSEC is contributing to security planning for major events and participating in security drills and exercises. Maritime contingency plans are under review by industry to ensure that they are effective and can be activated at all times.

7. The regulatory regime is being extended in two areas. First, by 1 July 2007 sea-going domestic maritime operations will come within the regulatory regime. Secondly and within a similar timetable, by way of an EC Directive, security regulations will also apply to all commercial maritime transport operations at ports, extending their scope beyond the port facility where the ship and the port interface.

8. Two considerations will help to lessen the impact of these legislative developments. First, domestic maritime operations will be subject to a risk assessment to determine which need to be subject to the full regulatory regime and those which may be exempted from some of the provisions. Secondly, the provisions of the EC Directive were foreseen and TRANSEC has tailored its existing instructions and guidance on security at port facilities accordingly.

9. The maritime security programme of TRANSEC also embraces operations which lie outside of the ISPS regime. The first step towards establishing this policy will be to undertake a risk assessment based on threat and vulnerability in order to establish the priority of further work.

Annex D

CONTINGENCIES AND RESPONSE

1. TRANSEC is mainly focused on seeking to prevent terrorist attacks. Response to incidents, as we saw on 7 July, is primarily a matter for the emergency services, working in close co-operation with staff from the utilities and local authorities (primary and secondary responders, as they are designated in the Civil Contingencies Act). TRANSEC is not the funder of any of these responders and is not empowered to direct their response activities. Nor would it wish to direct because it cannot be as expert in judging what is the best way to handle an incident underground, for example, as either the people who run the system or the highly trained emergency response personnel.

2. It does nonetheless have some important contributions to deliver. The aim of this work is to ensure that:

— at the strategic level, DfT plays its part in government-wide preparations for crisis and in exercises on contingency planning;

— individual divisions are ready to deliver what may be required of them in a crisis response (such as authorisation of air exclusion zones or relaxation of restrictions on drivers' hours); and

— there is dialogue with industry about contingency planning, so that TRANSEC can share information about risks and work together intelligently in a crisis.

3. TRANSEC also quality controls the emergency plans held by key divisions within DfT, setting out how they will deliver their part of a response to crisis, including one occurring without notice and/or "out of hours".

4. Ministers have agreed that it is not appropriate for the Department to audit transport operators' own contingency plans. However, TRANSEC has been stepping up contacts with industry on contingency planning to ensure that the transport sector has adequate information on developments (eg on current threats and hazards) to enable them to maintain, update and regularly exercise their plans.

5. Many contingency plans are regularly called into play to meet day to day problems such as breakdowns, bomb alerts or unplanned closures of transport systems. Along with partners such as the Regional Resilience Teams, TRANSEC seeks to add value at the higher level, where there is a need to ensure that plans consider wider events and indirect impacts. The value of exercises has been repeatedly mentioned by responders in debriefs following 7 July. These exercises not only model reality very accurately, but contribute to the familiarity and excellent joint working that was seen from all responders on 7 July.

Annex E

RESEARCH AND DEVELOPMENT

People screening

A major trial at Heathrow Airport provided successful results to the extent that TRANSEC approved the method as an alternative way of screening people, bringing benefits in terms of security and passenger facilitation.

X-ray screener competency

TRANSEC has made further advances in improving the standards of x-ray screening. A new version of the national test has been developed and introduced. This version has improved robustness and also raised the standard required. Further developments have taken place in the application of threat image projection (TIP)—a system for improving screener alertness. The UK requirements have been adopted by ECAC as the European standard.

Software which analyses the TIP data on individual screeners has been distributed to users. The process allows TRANSEC to monitor their performance and allow comparisons to be made between other UK airports.

Staff management

The supervisors of security staff have an important role to play in quality control. TRANSEC funded a comprehensive study into best practice, one output being a comprehensive guidance booklet. This new knowledge will be used to fashion a validation trial.

Technology evaluation

TRANSEC has continued to evaluate commercial security equipment in the areas of hold baggage screening, metal detection and explosive trace detection. The work on baggage systems has led to the setting of enhanced UK standards and, together with the work on metal detectors, has made an important contribution to the development of EU standards.

Witnesses: **Rt Hon Alistair Darling,** a Member of the House, Secretary of State for Transport, **Ms Niki Tompkinson,** Director of Transport Security and Contingencies Directorate, and **Mr John Grubb,** Deputy Director, Transport Security and Contingencies Directorate, Department for Transport, examined.

Q1 Chairman: I am delighted to see you this afternoon, Secretary of State. Can I just make a short statement. We are very grateful to you and your officials for coming to see us today on the important subject of transport security. I am going to ask you to introduce your colleagues in a minute, but I just want to say that transport security is a large and important subject, larger than we could do justice to in a single session. For that reason, the Committee will wish to conduct a full inquiry into transport security in the coming period. The single purpose of today's session will be to understand the Department's security function better and to determine what added value it can provide for keeping the travelling public safe, but I want to make it very clear to everyone taking part that the House *sub judice* rule prevents discussion in Parliament of specific cases which are currently before the courts. The aim of the rule is to safeguard the right to a fair trial and fair consideration of events at an inquest. Our questioning will take full account of the rule and it is of great importance that we have it very clearly in mind. Finally, I hardly need to remind you, Secretary of State, that the job of this Committee is to scrutinise the work of your Department, something which we try to do vigorously, but fairly, and I would like to place on record that we do understand the constraints on you and your officials in open session when discussing this subject. Equally, I hope you will feel able to provide the fullest possible picture of the work of Transec today. Secretary of State, perhaps you have got something to say to us before we begin.
Mr Darling: I do, Mrs Dunwoody, with your permission, but perhaps before I do that I could introduce my colleagues. Niki Tompkinson is the Director of Transec, the Department's transport security division, and John Grubb is one of her deputies. After I have made a few introductory remarks, I think it might be helpful if Niki were to outline her perspective to indicate the areas she proposes to cover, although of course we are happy to answer any questions within the provisos you yourself have established. I wonder, Mrs Dunwoody, before we get to that, if I could deal with one preliminary matter in relation to security because I think it is relevant to your consideration overall, and that is in relation to some tests and trials that we want to carry out on our mainline railways and on the Underground. You may recall that on 7 July and in the days afterwards I made the important point that you cannot run a closed system, as we do in the airports, on the railway system. In other words, you cannot have a sealed system where you are reasonably satisfied that

everybody going into the system has been searched, either their bags or themselves; it just is not possible. If you take the London Underground alone, it carries something like three million people a day and, again by way of comparison, Heathrow, as the Committee will know, is the busiest airport in the world and Waterloo Station carries four times as many passengers every day as Heathrow. I think if you just keep that in mind, people will accept that it is not practical to run a sealed system in any event with the mainline railway stretching over thousands of miles; it is not possible to seal every bit of it. That said, there is new technology becoming available all the time. The Department wants to make sure that, as and when new technology is developed, we evaluate it and see whether or not it would help us in reducing some of the risks that we know we have to encounter. To that end, I need to tell the Committee and, through you, inform Parliament that over the next few months we will be trialling various security equipment on different parts of the network. I am sorry that on Sunday somebody chose to leak part of it to a Sunday newspaper which has given rise to all sorts of wild speculation which is why I have said what I have said about the impossibility of having a sealed railway system. I am afraid that is what happens when you have to take a number of people in the industry with you before you make any announcement; somebody will go to the business pages of a newspaper and you just have to live with that. Perhaps I may just explain briefly what we are proposing to do. We need to test equipment and I can confirm that the first place we will be testing is in Paddington Station on the Heathrow Express. We will be carrying out further tests of different types of equipment at mainline stations and some tube stations.

Q2 Chairman: All mainline stations?
Mr Darling: Not all, no. What is most important is that we are not in a position to be introducing equipment across the network as we have in airports. This is testing individual equipment, some of it new to the market and some of it we have used in the past in aviation security. What we want to do is to see how it might work in a bus station, how it might work in a tube station, and bear in mind that these tube stations, for the most part, were built in the 19th Century, long before any of this problem ever arose, and obviously the environment in which some equipment works in an airport is completely different from the sort of environment that might work in a tube station in central London. Therefore, what we are doing is simply testing different bits of equipment that will come on to the market, some of

which has been developed and some of which is being developed, but what I want to emphasise again is, firstly, you cannot run airport-style security on the railways, tube or overground, and, secondly, the tests are alongside other security measures that we are taking, some of which are obvious, some of which are not so obvious, which we do not tend to discuss for perfectly obvious reasons. This is a commonsense approach. I think we would be open to criticism if new equipment came along and we did not actually trial it and ask ourselves, "Would it work? Could it help?" Immediately after the aftermath of the events of 7 July, there was one particular company appearing to suggest that they had kit which was ready to go if only the Department for Transport would buy it. That is not so. Equipment that can screen three million people a day without unduly inconveniencing them just does not exist at the present time here or anywhere else in the world. Therefore, what we are doing is simply testing this equipment. The reason I wanted to tell the House was that from time to time it will see this equipment, from time to time people will be asked to take part in these trials, to be screened and so on, and it is right that we should tell Parliament we are doing it. I will arrange for a fuller statement to be laid before the House tomorrow, but I thought it might be useful for the Committee to know this.

Q3 Chairman: Can I just ask you very briefly, you said the Heathrow Express, but is that both ends of the Heathrow Express, therefore, at Heathrow and at Paddington?
Mr Darling: No, initially it will be at Paddington Station.

Q4 Chairman: Anywhere else?
Mr Darling: This equipment will be at Paddington, but over the next few months, and I do not have start dates, we will be trialling equipment at other locations which we are still definitely to decide on. I should just emphasise again that this is not in place of what is there already. Some things will work, some things will not work, but if we do not test it, then we will never know. This whole business of how you reduce risk and have a grown-up discussion about these things, some things are possible to operate, some things are not, and I just want to test them over the next few months.

Q5 Chairman: Do we have any indication of how long the trials will last?
Mr Darling: We think probably about six months.

Q6 Chairman: Who have you consulted about this? Have you had talks with the Commissioner of Police?
Mr Darling: Yes.

Q7 Chairman: Also the Mayor of London?
Mr Darling: Absolutely, yes, and the Mayor, for his interest, is absolutely happy about this. He, like the rest of us, is determined that we should do everything that is reasonable, but the Mayor has also made the point that you cannot operate a completely sealed system as you do in the aviation field.

Q8 Chairman: Could you tell us who is going to evaluate the results?
Mr Darling: The Department will and from time to time obviously we will discuss with the police, we will discuss with London Underground, we will discuss with Network Rail, with the train-operating companies and various other agencies as well, but we want a thorough evaluation. The other thing of course we are discussing, and we continue to discuss, with the people who are actually developing this technology when new technology comes along is whether or not it is practical.

Q9 Chairman: I take it from what you have said that it would be some mix of existing technology and some experimental?
Mr Darling: Yes. I should also say that we will not always make an announcement before we do it because that would be self-defeating.

Q10 Chairman: Yes, but it just would be helpful for the Committee to know, and we assume there will be some indication, that if they are major stations Parliament will at least be given an indication of which stations will be involved.
Mr Darling: I can confirm that the first one will be Paddington and then as and when we have decided on other stations. What I cannot promise the House is that we will make an announcement in respect of every piece of equipment because there remain some things we want to test, but we do not particularly want to broadcast that we have that capability.

Q11 Chairman: Secretary of State, you have made the point very correctly, and we are now talking millions of people, not 10, that it is important to most major stations that passengers are not impeded.
Mr Darling: This is always the balance between making sure that people can go about their lawful business, people can travel, and reducing risk. At its extreme, the safest form of transport is one that is completely shut down and nobody can travel on it because not a lot can go wrong then.

Q12 Chairman: We have already tried that system!
Mr Darling: We have tried that from time to time and not always because of this particular threat. I think people would expect us to do things which are reasonable. People understand the risks under which we live, but, as I say, there will be things that we need to test and we will not be making a public announcement because we would be ill-advised to do so, but other stuff is perfectly obvious.

Q13 Mr Leech: You have half-answered my question already. Are you able to tell us what sort or any of the sort of technology that is going to be used?

Mr Darling: Yes. Some of the stuff that we will be testing is some of the stuff that we use at airports. For example, people will be familiar with the swab-testing we do of people's bags to see whether explosives have been used. Again it is useful to test that in an environment like a station where the air is of a different quality, shall we say, than it is in a sealed area. We will also want to look at screening equipment, what is practical and what is not practical. There is other equipment coming along that we will want to look at as well and this should very much be seen as sensible planning for the future.

Q14 Mr Leech: Is some of this technology stuff that people will not have seen at airports and elsewhere? *Mr Darling:* Well, it will be from time to time. I am grateful for that, but could I now turn to the subject of your inquiry and, before I ask Niki Tompkinson to say a few words, may I make some preliminary comments. Transec is a directorate of the Department for Transport. It is headed up by Niki Tompkinson who reports directly to me, although she is very much part of the Department for Transport. It is not an agency or anything like that, but it is very much a part of the Department and works with other officials there. It also works very closely with other Whitehall departments, with other agencies and of course with the various transport industries. Originally when it was set up, it was set up with very much aviation as the centre of its operations, but over time, for obvious reasons, it has expanded into ports and into railways, though the approach it adopts in relation to what it does will vary from time to time. I think it is important to emphasise that it is not a policeman; it is basically there to advise, to inspect, to make sure the standards are constantly reviewed and put in place and that they are actually operated. It can only work with the full co-operation of other agencies and other industries, which it does quite well. You will have questions, which we will answer, on the budget and the number of staff, but what I would say to you, Mrs Dunwoody, which may be of help to your Committee, is that when I became Secretary of State just over three years ago, it was an important part of the Department, but it did not take up over-much time. In the last few years it has become an increasingly important part of the Department and takes up an increasing amount of my time. I think it would probably be appropriate at this stage, if it is okay with you, to ask Niki Tompkinson perhaps to give an overview of what she does and then we can take it from there.

Q15 Chairman: Yes, exactly right, Ms Tompkinson, would you do that for us please. *Ms Tompkinson:* I will try to keep my opening remarks brief because I know you have read the memorandum that we sent along ahead. I thought perhaps I could make just four points to begin with which outline the priorities that Transec has been working to since 9/11, which was the watershed, I think, for those of us who work on transport security. There are four things we have been focusing

on. The first is to maintain and to develop the security programmes that were already in place at that time and we have continued to build on those. I think it is fair to say that we started from a position of strength on 9/11; we already had very well-developed and regulated programmes, particularly for aviation, as the Secretary of State has remarked, and we also had some security in place for passenger ships, particularly the cruise ships, and we were already giving advice and guidance to the rail and Underground networks, so those programmes were there and we have been able to build on them. Domestic aviation, which was our focus then and continues to be a prime focus for us now, was really a model for other people and that has been one of our strengths. We continue to put an effort into maintaining that and other programmes and adapting them to new circumstances, so one of the pieces of work we have to do on a regular basis is to continue to review what the threats are, what we know about them and whether our current programmes are fit for purpose, and that takes quite a lot of our time. After 9/11, there was not really a great leap forward in terms of our domestic aviation programme, but a stronger focus certainly on in-flight security was the main lesson that came out of that. I would say at that time and now, standards of compliance were good. We already had an inspection regime in place that indicated that and, since then, we have had a number of outside audits and we have had Sir John Wheeler's review in September 2002 which endorsed our programme on aviation. On the international side, this is an area where we have actually increased more than on the domestic focus. Increasingly, we have felt that we needed to give more advice and guidance to airlines and to the shipping industry in their overseas operations, and we have now quite an extensive programme in place with a number of individuals posted overseas to advise on transport security in the regions where they are based. We have also put more resource into working with international bodies, such as the International Civil Aviation Organisation, and with the European Commission to raise standards worldwide, so all of this is part of doing what we do, our professional work, and making sure that we keep the standards high. That is the first point. The second point is we have put a lot more focus on to new programmes, which has been another key priority since 9/11, the work on the maritime programme, for example, the work that was promoted by the UN, the International Maritime Organisation and by the European Commission to extend the regime, which we already had in place, to cargo and other ships. There is also a new dangerous goods regime which has come in in the last year or so. Since Madrid, the bombings in Madrid, and the events this year in July here, there of course has been an increasing focus on our rail and Underground systems, the soft targets that we have there, and in that respect we have now formalised the informal regime we already had in place and those industries are now subject to formal regulation. We have kept this under constant review since Madrid and a further review after July. The third point I just

wanted to make briefly is that a key focus for me and my team has been to build Transec in order to build all this work; it could not have been done without that. We inherited a strong team, I think, just after 9/11, people who knew their business very well, and we wanted to build on that, but we have increased from a staff of 81 to 200 now to do that work. Finally, again a point that I think the Secretary of State has also made, the key focus for us is to strengthen our links to other agencies. We do not work in isolation, we never have done and we certainly do not do now. We cannot ring-fence just our activities as being the only way to deliver transport security, so we have been building increasingly close links and synergy with others, particularly the border agencies, the police and customs, as well as of course our very good relationship with the industry itself. That really is just to set out my stall, if you like, the areas that I have been focusing on, and I am happy to take questions on any of that.

Q16 Chairman: You have mentioned railways and the Underground, both of which of course are "soft targets". One could say that with the terrorist attacks on 7 and 21 July, we got it wrong and we have actually failed.

Ms Tompkinson: I would not say that we have failed. I think those attacks, terrible as they were with the number of deaths and injuries caused, were the type of attack which it would have been extremely hard to avoid anywhere on any system in the world. Our focus on the Underground and rail has been on other types of attacks to ensure that other sorts of security are in place. One of the things that we constantly remind ourselves of is that whatever the attack is today, there have been other types of attack that we need to protect the transport industries from and we cannot just focus on the one that has happened and there are things that we do which will prevent other sorts of attack.

Mr Darling: I would just make one point in relation to the Underground. I am quite clear that one of the reasons that the emergency services and the people working on the Underground were able to respond so well on 7 July is because of the training and the exercises that were carried out in the preceding few years, and also because three years ago we were concerned about the ability to conduct that sort of rescue. A lot of expense was incurred and effort was put in to improving the equipment that the emergency services carry. Of course I accept that that is dealing with the aftermath of an incident, but, from my own observations, had this happened three years ago, then of course the men and women working in these services would have performed heroically, as they did, but their preparedness was much better than it was and I think that is an essential part of what we do. For Transec, part of its job is to look at this response and to ask, "How can we make this better?" as well as of course looking at things that can deter and prevent these attacks taking place.

Q17 Chairman: Have you in effect made your training programmes better and improved on them since then?

Mr Darling: Yes, I think all the emergency services after 7 July had, as you would expect, the debrief to look at what could have been done better and I think that process is continuing in that they have not reached a concluded view there, but I know that three years ago a lot of the kit they actually carry now just was not available. There is a huge amount of work which has gone on sometimes, I must say, rubbished by commentators outside when we test these things where people have said, "Look, there isn't a risk. You're just exaggerating these things", but I am very glad we did that work because I am quite sure it has contributed to what I think, on any view, was quite a heroic effort on 7 July and in the days and weeks after that.

Q18 Mrs Ellman: In your memorandum, you talk about achieving a balance between security for the public and burdens on industry. How do you assess where that balance lies and is it not a concern that if decisions are taken on a commercial basis, it is likely that security will be at risk?

Mr Darling: No, and I will ask Niki to say something in a moment about that on the operational side. What that means is, as I was saying earlier, you have to strike a balance between what is a reasonable proportion, what is a reasonable position, if you like, on passengers and on an industry and where you tip over into something that is just unreasonable and is causing so much inconvenience that it is not worth it. For example, I will use the example of screening which is now commonplace in every airport around the world, but 30 years ago there was a big debate as to whether or not that was a big imposition on people to have to go through detectors or it was an imposition on the industry to put that in, but most people think that is perfectly acceptable. You can imagine a situation where you could introduce more screening, perhaps 20 minutes per passenger to screen them, and you say, "Is it worth doing that? Would you actually find something? Is it worth virtually bringing an airport to a halt by doing that?" These are judgments that you have got to exercise all the time, but I can think of no instance where people have said, "Well, actually we would really like to do this. It would be really first class, but it's too expensive". It is a judgment reached, there is no science behind it, it is really a commonsense judgment.

Q19 Mrs Ellman: Are you saying that there are no instances at all where it was felt that, for security reasons, something should be done and, for commercial reasons, the operator concerned did not want to do it? They may not have put it in that way.

Mr Darling: No, I cannot.

Q20 Mrs Ellman: It may have been an underlying reason.

Mr Darling: I can think of many cases where the operator has groaned and said, "Surely you don't expect us to do this", and we have said, "Yes, we

do", and they have done it. For example, now in more and more airports we insist on segregation of incoming and outgoing passengers, and that is expensive because it means you have got to build basically two corridors. Of course the industry will say, "That's expensive and we've got to find that money", but we take the view, "Well, you've got to do that because we think that's sensible". Maybe we have not been in a situation where we have thought of something which we think is so good that we should do it and the industry is saying, "Well, it's out of the question because it would cost trillions of pounds", and so on, but at the end of the day we are all on the same side in this, whether an airport operator, for example, or a train-operating company, the Government, Transec and so on, and we try and do things which are sensible, which are proportionate and which work. There is no science to this. You cannot do a nice calculation and come up with the answers and proceed on that basis, but you just have to exercise a degree of commonsense, I think.

Q21 Mrs Ellman: Transec can only make recommendations, can it not, so do you think there is a case for strengthening it?
Mr Darling: No, we can tell people what to do.
Ms Tompkinson: We can indeed tell people what to do because we issue directions to the industry which do require them to carry out the measures that we have advised. To come back to your earlier point, the way we manage it is to work very closely with the industry, so we are trying to develop some new measures, for example, and we do not just sit down and do it on our own, but we will work with the industry. We share the problem with them, brief them on the threat, make sure they understand the sort of threat that they might be under, and then we can work with them to try to devise a measure that will meet that particular risk that we all share.

Q22 Mrs Ellman: Are you working with airline manufacturers and looking at design materials to withstand explosions?
Mr Darling: That work goes on all the time. I think Transec will naturally take an interest in that, as do airlines, as the purchasers of a number of these aircraft, and ourselves, but yes, we do and all the time the manufacturers are coming up with a better design not just against any explosives, for example, but also the better design of aircraft to deal with the normal conditions they encounter.

Q23 Mrs Ellman: Transec has a lot of different organisations in it, has it not, but do those work well together and how well is that linked to the Security Service?
Ms Tompkinson: Transec is one organisation, not a mixture of organisations. It is one part of the Department, so it is just a separate directorate. People within Transec come from either elsewhere in the Department or from other departments or from outside where we recruit people from industry. We are all there as mainstream civil servants as part of the Department and we are not a mixture of

organisations. We work very well with the Security Service and other intelligence organisations, and that is a key part of our work, to make sure that we understand the sort of threats that they can describe and assess for us, so that relationship is a very close one.

Q24 Chairman: Could I ask you whether you would be surprised to hear that British Airways said that to their knowledge, "no regulatory impact assessment has ever been undertaken to demonstrate that the additional requirements are either proportionate or reasonable to address the assessed threat. If such an assessment has been undertaken, its analysis and conclusions have not been shared with the industry, nor was it consulted"? In the light of what you have just said, does that surprise you?
Ms Tompkinson: I think it does surprise me hearing it like that. Formally, yes, they are correct, we have not gone through the sort of process which I think you are describing there, but the work that we do with the industry would always take into account whether or not they say they can deliver it because our view is that there is no point asking them to deliver a measure if it is going to bankrupt them or they simply cannot do it, it is not doable. It comes back to finding out what can be done and what cannot, and we are working with them to an accommodation. As we have said already, this is not a science, it is an art, and when we are discussing with the airlines, the airports and all the other industries what to do, we are very interested in the end objective, and then there will be different ways of meeting that objective, so we might start off with one idea about how we might meet that objective and the industry might have an alternative idea which would be equally good and we would be very happy to go with that as well.

Q25 Chairman: It just seems to be a little bit surprising in view of what the Secretary of State said, that they could not actually recall a regulatory impact assessment.
Mr Darling: Well, I am not surprised at that. If you look at the way this has evolved over the years and increasingly over the recent years, it tends to be at each stage, at each development in the light of threats and in the light of actual incidents that security has been tightened. Therefore, we have not, I think, carried out a formal regulatory impact assessment and I just wonder what we would actually find if we did one. I may say that, on most occasions, most British airlines are more than happy to co-operate with the sort of things we have developed because, as I said earlier, I think, in reply to Mrs Ellman, we are actually all trying to achieve the same end and there is a premium on airlines doing as much as they can to make travel safe because that gives their passengers confidence.
Chairman: I think what everyone feels if they are of general intelligence is that they probably did not perceive that.

Q26 Mr Clelland: If we had been having this discussion before 7 July, then the description that you gave of well-developed and regulated programmes might have instilled some confidence among the Committee, but we now know of course that they were absolutely no use to us at all on 7 and 21 July, so why should the Committee have confidence that these well-developed and regulated programmes will be any more efficient in the future?

Ms Tompkinson: The answer to that is that our programmes are very sort of wide and varied. The events of 7 and 21 July were specific circumstances, an attack on a local network which, as I said, is probably the most difficult one to prevent at the time that it happens, but that does not mean to say that the other measures that we have in place are not valid, but we have to take into account other types of attack and other threats to the network, whether it is a closed network like aviation or the open network. Of course what is never known, and it makes it very hard for us to assess the success of our job, what is never known publicly, and we do not know either, is what has not happened and what attacks have been prevented. That is a completely open question.

Mr Darling: I am not sure I share the analysis behind your question. Yes, it is true that these attacks happened and it is patently obvious that it was not possible for us to forestall these attacks in the first place and, as has been said on many occasions before, a terrorist only has to be lucky once. There are, as Niki has just said, a number of occasions when we can be reasonably confident that things that we did stopped things happening, although it is very difficult to prove a negative, if you like, and it is extremely difficult to prove when we cannot discuss these things in open court, as it were. If you are operating an open network, like the tube or the mainline stations, what you are aiming to do is to try and cut down the risk as much as you possibly can through intelligence, through conventional policing, specialist policing, measures that we impose on the operators and so on, but, as I say, what you cannot do is seal off the system from attacks completely. You cannot do that short of shutting down, which I do not think anybody would advocate at all, but that is not to say that we cannot improve and we cannot do better and each day we try and do that, but I think we are very aware that we are living under a very different risk from the one that we have lived under for the last 30 years with Irish terrorist groups and so on, and I am afraid it is one that we are going to be living under for the rest of our lives and probably our children's lives as well. We just have to make sure that on each and every occasion we learn from what happens and we try to shut off options, but, remember, there are people out there who, if you shut down one option, are looking for another one and that is just something we have got to be vigilant about.

Q27 Graham Stringer: Does the Government have a view on extending the use of mobile phones and the technology required to use mobile phones into the Underground system?

Mr Darling: Yes, and here there are two things. One is that we are looking at the lessons which have been learnt after 7 July with mobile phones and I think it is common knowledge that in the immediate aftermath of those attacks, just about everybody in London and everybody who had a relative or a friend in London got on their mobile phone, but the network can only take so much and we need to look at that. There are a number of steps which are on the way which will, I think, help us if we are faced with a similar situation in the future. The point about the Underground itself is that, as you know, the attempt to replace the communications between control rooms and trains with a PFI contract ran into all sorts of difficulties. However, that contract, which has been operated by TfL, has now been reconstituted and I think they are confident that by the end of 2007 there will be a new system in place which will allow them to have a far more up-to-date and better communication system than they have at the moment. I may say though that on 7 July itself, although there were some difficulties, that was not in itself a major difficulty that the emergency services had to face. Once they were clear what had happened, they were able then to get on with it and deal with it and they were able then to put temporary arrangements in to restore communications, especially in some of the tunnels where the explosions had disrupted the communications that otherwise were working. Niki, is that a fair summation?

Ms Tompkinson: Yes, I think that is right.

Q28 Graham Stringer: That was very interesting, but it is an answer to another question which I might have come to. What I was thinking about was extending the technology so that you and I could use our mobile phones in the Underground and that technology might be used to trigger a bomb to go off if you were to allow the radio waves to go down the tunnels. Does the Government have a view about the extension of that to be able to use mobile phones?

Ms Tompkinson: Again it is a balance and, yes, it is one way of triggering a bomb, but it is not the only way and there are plenty of other means of triggering a bomb. You balance that against the benefits that there are to people if they can use their mobile phones on the Underground, not least of which is that, if there is an incident, people need to contact other people, so I think from a security point of view I would not put up a case to prevent the use of mobile phones on the Underground, no.

Q29 Graham Stringer: Are you satisfied with the quality of the coverage of the CCTV in the Underground system?

Mr Darling: The answer to that is that it is being upgraded at the moment. We have had to move very quickly. Post Madrid, I think there was a realisation that we need to have modern and up-to-date CCTV in most parts of the network and there is a plan underway to do that which London Underground are putting in place. As you will know, because of the legacy arrangements, there are many different types of CCTV where some are pretty old-fashioned and

some are very modern and very, very good. There is a general plan to upgrade them both on the Underground and on the mainline stations and in other places where we think we need to do that, but I think the answer to your question just now is that improvements are being made, but an awful lot more improvements need to be made in the future.

Q30 Graham Stringer: Is there a schedule for those improvements?
Mr Darling: There is a programme to work through. Both Network Rail have one and London Underground have one as well.

Q31 Graham Stringer: When will the system be to the Government's satisfaction?
Mr Darling: The answer to that question is it probably never will be because, as more and more kit comes on to the market, you want to get better and better stuff. Again without going into detail for obvious reasons, there is CCTV that can do things that two or three years ago would have been unimaginable.

Q32 Graham Stringer: Can I ask you, on a completely different point, Secretary of State, whether you have read the 9/11 Commission's report? It is probably the most frightening report I have ever read, very clearly written, and it showed that there were all sorts of communication problems within the United States between the different agencies there and air traffic control and the defence system. Can you assure us that in a similar situation, were it to happen in the UK, the British Government has learnt from that and that there would be good communications between the different agencies?
Mr Darling: Yes, and obviously it is not just this country we look to and incidents that we have had over the years, and of course we look not just at the United States, but there have been many incidents around the world. I suppose, Mr Stringer, one way of answering this, without being complacent in any way at all, is that on 7 July we were able to respond very quickly once it became apparent that there had been these attacks because we have tried and tested in exercises as well as sometimes in incidents bringing people together, the key agencies, both ministers and people from the police, the emergency services, the transport operators, bringing them under one roof under the COBR system. We were able to work very closely together to be able to discuss what was happening and how we respond to it, how, within an hour of the attack, we were planning for the recovery and so on, and all these things could be done because we had brought the people together. Although, if you look at a sort of chart of who does what in Whitehall, you might come to the conclusion that there seems to be a lot of different bodies doing different things under different chains of command, in practice it is not quite like that and all these services work very closely together. One advantage I think we have got which the United States did not have then, and it is getting a lot better now, is that the United States had a lot of agencies that were fairly freestanding and fairly

independent of each other and some of them jealously guarded their independence. I think on an occasion like 9/11 or any other, this is not the time to be standing on ceremony; you are in it together. I think although there are lessons we need to learn after 7 July and there are improvements that need to be made which we could identify on the day needed to be looked at, I think, generally speaking, our response was seen by people in this country and also, incidentally, by the United States, especially in the light of their recent experiences and civil problems in New Orleans and so on, and they have been asking themselves, "How do we better organise central government and its agencies to pull in the same direction?" Now, I am not being complacent and, yes, there were problems, but it was striking how, by the fact that in this country we can get people under the same roof very quickly, you can actually make things happen quickly.

Q33 Graham Stringer: That answers the question really about training, and you did not mention air traffic controllers, but you think that it was a similar scenario to 9/11?
Mr Darling: Yes, absolutely.

Q34 Graham Stringer: Okay, I accept that. In an equivalent situation to 9/11, are you confident that all the IT systems are up to communicating across the different agencies and making sure that there is a unified response?
Mr Darling: Well, I will ask Niki to talk about the IT. The day we all have the same IT for everything is probably a very, very long way off for obvious reasons. I think what you need to recognise is that there are some things that IT is important for, for communication, and there are other things where there is no substitute for word of mouth and actually having people sitting in a room, talking to each other and saying, "What do we do? What's happening? How do we react to these things?" As I say, we are always looking at these things, always testing, and just about every month there is a separate exercise going on, testing these things, and that does actually sometimes expose difficulties. Niki, do you want to deal with the IT point?
Ms Tompkinson: Yes, the point to make is that obviously increasingly people are dependent on IT systems to operate and to communicate with each other, and those IT systems can themselves be threatened, so they can be vulnerable. There is an organisation within government which exists purely to advise industry and critical national infrastructure on their IT security, so we do not have the expertise in Transec, but it is an organisation that we work with and it is within the Security Service. They have the expertise there and they work directly with the industries to advise them about these systems and they can put out alerts if they are aware of any particular threats or viruses that are coming.

Q35 Mr Donaldson: Intelligence has already been established as being an important element in thwarting terrorist attacks. Indeed our experience in Northern Ireland is that, through intelligence-based

counter-terrorist measures, we were able to thwart four out of every five terrorist attacks in the Province. Therefore, what steps is the Department and also Transec taking to ensure that there is close liaison with the Security Service on the question of the flow of intelligence to your organisation?

Ms Tompkinson: The flow is very good indeed and very immediate. The threat from international terrorism is assessed by an organisation called JTAC, the Joint Terrorism Analysis Centre, which is a number of different organisations which have come together to form the definitive assessment of the threat from terrorism. Within Transec I have a small threats team who liaise directly with JTAC and indeed they are double-badged, if you like, in that they are members of JTAC as well as members of Transec, so they sit in Transec all the time, but they go regularly, daily, to JTAC to receive intelligence briefings and they have direct access to all of the intelligence, and we can commission assessments and we can ask for clarification of any of the information we do not understand. It is a very close link, so my threats team have a link between the intelligence agencies and the rest of Transec, and if there is new threat information, we get it immediately and we can then translate it into, "Do we need to respond to this? Is there something we need to do? Who do we need to talk to in industry? What are the measures we need to take?" It is very quick and that operates 24/7.

Q36 Mr Donaldson: What is the current intelligence assessment of the present level of threat from a terrorist attack to the UK transport system?

Ms Tompkinson: I do not think that is a question for me to answer in this forum. Clearly since the attacks in July it is well known that the threat remains very real, as it did before, and we need to take all measures to counter that.

Q37 Mr Donaldson: How much credence do you place on intelligence assessments that come to Transec?

Ms Tompkinson: We place very high credence on them, but we understand that again intelligence and the assessment of intelligence is an art, not a science, so you know what you know and the assessments are made with the best possible expertise and in the light of all the information that is available.

Q38 Mr Donaldson: To what extent is security at airports, and particularly airports in the UK that deal largely with domestic passengers, influenced by those intelligence assessments?

Ms Tompkinson: The regime that is in place at airports is standard at all airports, so we do not have different security in place for domestic as opposed to international, so they all operate the same regime. We have a layered approach to security, so there are basic security programmes in place and then additional layers of security on top of that and that is where we are at present because we consider we are at a heightened threat from terrorism. We can adjust

the measures if new information comes in, but essentially it is the same across the board at all airports.

Q39 Mr Donaldson: You say that, but if I am a passenger travelling from London to New York, I join a queue to go through the security system and all the passengers have the same experience. However, if I am at Liverpool Airport travelling to Belfast, I have to join a different queue because I am going to Northern Ireland and I have to go through an entirely different security check where my photograph is taken, whereas if I am a passenger travelling to Glasgow, my photograph is not taken at Liverpool Airport or at Manchester Airport, so how come at the domestic level you have a different regime operating at many of the domestic airports in the UK which treats Northern Ireland passengers separately and differently and at a higher level of security than for the passengers travelling to other UK internal destinations, if, as you say, the level of security is the same for domestic and international passengers?

Ms Tompkinson: The regimes that I am talking about are the physical security regimes that we regulate and they are the same for all airports. There may be additional measures in place, and I mentioned earlier that we work closely with the control agencies, the border agencies, such as the police, immigration and customs, and they may have different requirements which may be over and above or different from our own, and that might explain some of the different measures that you see. However, in terms of DfT's programme that we require of the industry, it is uniform throughout all the airports.

Q40 Mr Donaldson: So are you saying that Transec at the moment does not require airport security to take photographs of passengers travelling on internal journeys from one UK airport in Great Britain to another UK airport in Great Britain?

Ms Tompkinson: It is not one of our requirements, no, that is correct.

Q41 Mr Donaldson: Do you not think that needs to be reviewed?

Ms Tompkinson: Well, it is not my requirement. Are you saying that we should be doing it to all passengers or that we should not be doing it to some?

Mr Donaldson: I know we have had a problem in Northern Ireland, and thankfully most of the problem has gone, but I am not aware, for example, that al-Qaeda operate in Belfast and, therefore, that there is a particular risk from an al-Qaeda attack on a flight from Belfast into Liverpool, Manchester, London or any other UK airport. Therefore, I am asking you why it is deemed necessary only to photograph passengers travelling to and from Belfast and not to photograph other passengers and do you believe, therefore, that the risk of a terrorist attack from Glasgow, say, to London or from Leeds to London is less?

Q42 Chairman: If it would be helpful at some point, perhaps you could actually give us a brief note in confidence about that.

Mr Darling: I would make an observation here. Niki is making the point that a Transec requirement is not for photographing. What she is saying is that there may be other agencies who may be very interested in who is flying into Belfast for reasons that you will be more aware of than I. However, it is not our policy at the moment to photograph people going from, say, Edinburgh to London. I may say for the sake of completeness, because some of you may have observed this, that there are a number of airports where an enhancement of security when you go through the security check at Gatwick and Birmingham, for example, is that you are photographed and it is on a bar chart, so they can see it is the same person going on to the aeroplane as the one that checked in through security. The reason for that is with airports being large shopping centres with all sorts of people milling around, it is quite a useful thing, but, no, we do not insist on everybody being photographed. Obviously these are things that people consider, but I think there is a specific reason for being very interested in who is flying across the Irish Sea and I think you will know why that is.

Mr Donaldson: I understand that, Secretary of State, but I am somewhat surprised that some of these measures have only recently been introduced when it is clear that the threat in respect of domestic terrorism is significantly less now than the threat from international terrorism.

Q43 Chairman: I think the Committee has a right, Secretary of State, to ask you about the security treatment of passengers going through domestic airports.

Mr Darling: Of course it has.

Q44 Chairman: We would welcome a note on that.

Mr Darling: If you would like a note, we can certainly do that.

Q45 Chairman: I think it would help.

Mr Darling: I think we had better check with the people who might be requiring these photographs.

Chairman: Yes, but we just need a clear explanation of this.

Q46 Mr Scott: Secretary of State, are we liaising with other countries who have experienced homicide bombings, particularly on buses, and do we liaise with their agencies as well and take some advice on perhaps some techniques they have? I am thinking of Israel who have experienced this for many, many years.

Mr Darling: Across government, and indeed Transec, we do keep in regular contact with their counterparts and from time to time it may be specific incidents or it may be things in general which are discussed because quite obviously we should learn from their experience. Sometimes there are direct lessons to be learned, sometimes there are not.

Q47 Clive Efford: Could you explain why the annexes breaking down Transec's total running costs, expenditure, programme expenditure and human resourcing, which feature in the annual reports of 2001 and 2003, have been dropped in the 2002 and 2004 reports?

Ms Tompkinson: I think when we did the more recent report we felt that perhaps too much detailed information had gone into the earlier reports and particularly now we wanted to get something that we put on to our website which would be very accessible to the general public. If you would like to see that detail of information again for the current years, then we would be very happy to provide that if it would be useful.

Q48 Clive Efford: Is it an onerous task to produce that material?

Ms Tompkinson: It is not particularly onerous, no. It is another job to do and it is the sort of work that we would do in-house. We were trying to strike a balance between getting information out into the public domain on our website and what we thought would be of interest to the public and relevant to their interests and maybe it was at the expense of providing information which would be of use to this Committee.

Q49 Clive Efford: Your business plan is security-classified and not publicly available?

Ms Tompkinson: That is correct.

Q50 Clive Efford: How can we be assured the format accords with best practice?

Ms Tompkinson: As the Secretary of State said at the beginning, my directorate is very much part of the Department, so within the Department I am subject to all of the usual rules and regulations and oversight of any part of the Department. I have to produce an annual business plan according to exactly the same criteria as other parts of the Department, the only difference is it is classified because of all the material we bring together and it will tell you something about the vulnerabilities we perceive which we are working on. The management board looks at all of the directorates' business plans, it certainly looks at mine. We have to put in a return every two months to say how we are making progress against some of the key items, and I have regular meetings with the Director-General I work to within the Department and the Permanent Secretary to assure them the work is in hand and being completed.

Q51 Clive Efford: So your department is treated exactly the same as others? For example, you have departmental targets?

Ms Tompkinson: Yes.

Q52 Clive Efford: Is Transec's work included in the public service agreement for the Department for Transport?

Ms Tompkinson: There is not a public service agreement for Transec's work, no.

Q53 Clive Efford: Is there a specific reason for that?

Ms Tompkinson: I will have to take advice on that within the Department. I will have to give you a note on that.

Mr Darling: We do not have a public service agreement for every single thing we do and I am not sure this is an area which readily lends itself to that, but if your Committee were to come to the view we ought to have one, I am sure we could add it to the list of the ones we have.

Q54 Clive Efford: It is an area we might explore in our report. Secretary of State, Transec has 200 staff currently, which seems quite modest compared with the growth in demand for work in the area of security on transport. Are you confident that is a sufficient number of staff? If not, what do you intend to do in the future to address that?

Mr Darling: I made the point at the start that Transec does not operate on its own, it uses other agencies, other parts of the Government, and Transec has increased in size quite dramatically over the last three or four years. If there was a case to be made for employing more people to do activity, that would be something we would certainly look at. I suppose that is an area where you would have to agree with me, Niki, but as far as I know you are very happy with your staffing levels.

Q55 Clive Efford: I was going to ask that. Are you completely satisfied, Ms Tompkinson, that you have sufficient staff and the correct skills base to fulfil the role? If not, in what areas do you feel you need more staff and more trained staff?

Ms Tompkinson: I am satisfied with the numbers we have and Transec has been ring-fenced within the Department alongside the Accident Investigation Branches. We have been ring-fenced in terms of any headcount exercises, so we have not had to make any cuts at all. Our establishment of 200 has been preserved and if I need more I know I can make a case and bid for it, and that would be scrutinised alongside other bids.

Q56 Chairman: It may be ring-fenced but if you are 0.125% of the budget of the Department, they are not taking an enormous risk in ring-fencing you really, are they?

Ms Tompkinson: In terms of the current scrutiny of headcount within the Department, yes, we are now quite a considerable proportion of DfT Centre, which will be a fairly modestly sized central department of about 1,700, of which we are about 200, so that is quite a large proportion. In terms of the skills set, we recruit people into Transec who either have the right skills or can be trained in our sort of work, and I ensure we do not take risks by bringing people in who I think are not up to the job. So our recruitment process is a very careful one.

Mr Darling: It is a fairly specialist unit. The point about ring-fencing is important because, as you know, all government departments are required to reduce their general Civil Service headcount, but Transec is exempted, because it is a front line service, and patently it would be unwise to be reducing the

staffing there. It is quite important. It did not have that security even 18 months ago. It is relatively recently we got this agreement with the Treasury but it is quite important in terms of the work being carried out.

Q57 Clive Efford: How do we compare with similar organisations overseas in terms of size and skills?

Ms Tompkinson: Most of my opposite numbers overseas are envious of the amount of resources I have.

Chairman: I think, Ms Tompkinson, you are ruining the future of your unit.

Q58 Clive Efford: You are forgetting that between 1994 and 2001 your department was reduced in size by about 20%, so perhaps that was not the best answer. Are all your staff permanent or are some seconded?

Ms Tompkinson: They are mostly permanent. We have a few secondees who come in and do a specific job and then leave again but the vast majority of the staff are permanent.

Q59 Mr Martlew: I have been very impressed with your presentation and it appears you are upping security especially on the Underground and we talked about the new facilities being tested out at Paddington. If you look at the terrorists we are dealing with, they go for the soft target, and I am not saying you should not be doing this, but I have a concern that perhaps too much of the concentration is on London and on the Underground. We have a Metro in Newcastle and a tram system in Manchester. If the terrorists are going to go for the soft option, surely they will move away from the Underground, which is fine and I do not disagree with that, and they will look at these other vulnerable areas. A perfect example is that everybody has buses and there was a bomb on a bus.

Mr Darling: I was conscious just before you spoke that this has been a very Londoncentric discussion so far and it is important to emphasise everything we have said so far applies to the transport network the length and breadth of the country. Obviously in aviation, which we touched on with Mr Donaldson, once you are in the system, you are in the system, so we are interested whether you get on at Heathrow or get on at Stornoway. In relation to the Underground system, the Glasgow Underground is regulated; it is a fairly recent thing we have introduced but it is treated in the same way as the London one in terms of the attention we give to it. As is publicly known, there have been terrorist activities in cities outside London and we do work both as a department and also as Transec within the Department for Transport with local authorities and with police outside London. You are absolutely right, you cannot assume that any part of the transport network is immune from attack, you have to proceed on the basis there is a risk right across the network no matter where it is. Indeed some of the measures we are currently contemplating in relation to railway stations will cover stations well away from London.

Q60 Mr Martlew: Just on the bus side, the point was made before about attacks in Israel and we did have one of the four attacks on a bus, is there enough effort going into that?

Mr Darling: It is something again we keep constantly under review. For example, a few years ago CCTV on buses was pretty rare, but London will have very shortly all its buses with CCTV and outside London increasingly new buses come fitted with CCTV. I am bound to say it is mainly to stop hooligans and vandals but it serves the same purpose. We are acutely aware of the risk. We are also aware, and this comes back to the discussion with Mrs Ellman and Mrs Dunwoody at the start, it would be rather difficult to screen everybody before they got on a bus. In Israel they have particular measures which include soldiers on buses but, as we can see, no matter what you do there will always be a risk.

Ms Tompkinson: On the point about what do we do to find out more about the whole question of suicide bombers and what can be done, that is very much a matter for the police and I know they have done a lot of work with colleagues overseas, and Israel is a case in point. We have spoken to Israeli counterparts briefly on this but there is a lot of work going on to look at suicide bombers which could manifest itself not just on the transport network. In terms of buses, we have recently put out some written guidance to all bus operators which is based very much on the programmes we run on the rail and Underground networks, so they have some security guidance and best practice to work to. I think we will be doing more of that over the coming months.

Q61 Mr Martlew: Earlier, you said your guidance was instructions, that you had the right to do that, is that what you are doing with the bus companies?

Ms Tompkinson: No, we do not have powers to give instructions to bus companies, whereas we do on the rail and Underground, and we have taken powers to be able to extend that to the light rail systems, to the tram networks.

Q62 Mr Martlew: Are you thinking of extending it to buses as well?

Ms Tompkinson: We are certainly thinking about it, yes, we are.

Q63 Chairman: Bus companies are not open to a lot of persuasion.

Mr Darling: It depends.

Q64 Chairman: There cannot be that many wanting to get to the House of Lords, surely?

Mr Darling: If you take the CCTV, an increasing number of bus companies can see the merit of having it for non-terrorist reasons, and there are other things we want to encourage too. If we think we need powers to tell people what to do, we will take them.

Chairman: We will remind you of that.

Q65 Mr Goodwill: On 9/11 the buildings withstood the impact of the aircraft, it was the fuel fire which actually brought the buildings down. Having worked as a tanker driver and trained in hazardous chemicals I can imagine probably better than most the effect of a chemical attack or a fuel tanker being driven into a building or exploding in an area of high population. Given we have in the region of seven vehicle hijackings a month and it is much easier to hijack trucks than it is aeroplanes, have you assessed the risk to people from vehicles being hijacked and looked at areas such as better secure parking overnight for tankers, a clamping down on the way people can obtain operators' licences by unconventional methods and better checks on drivers and driver training schools to stop this one happening?

Mr Darling: We have discussed this a lot. I will ask John Grubb to comment on this.

Mr Grubb: We have recently introduced a system of regulation for the transportation of dangerous goods and high consequence goods, which includes the tankers you mentioned. That does include the development of security plans which are both how these tankers are handled in the depot and what you can do on the road, which is of course limited, but it does include secure overnight parking and arrangements when these vehicles might be left in a situation where they might be vulnerable. We do have a system of compliance now with the Department's Vehicle and Operator Services Agency for spot checks to see these arrangements are in place. It does include making all the background checks you can do on drivers and satisfying yourself as best you can. There are also arrangements which we have discussed and agreed with the police as to what we might do in a response situation where a tanker may be hijacked and you cannot obviously foresee that, and that is what we have just recently done and published.

Q66 Mr Goodwill: Are you aware of the unconventional means which can be utilised by some companies to obtain operators' licences? For example, one company goes out of business and they sell the limited company along with the operator's licence. Maybe the Secretary of State would like to look at that and clamp down on that. There are these licences which are being advertised openly in the commercial press.

Mr Darling: We are and this is something which VOSA, which is the appropriate agency in the Department, is very aware of. For every reason you can think of, that sort of activity needs to be stamped on, not just because of terrorist implications but because it is bad for the industry generally.

Q67 Graham Stringer: I wanted to follow up on your answer to Mr Martlew's first question, that when you get on any aeroplane you are in the system, and previously you talked about aviation being a closed system, but it is more closed in parts of the system than other parts, is it not? If you get on at Heathrow, Gatwick, New York, there is tight security, if you get on an aeroplane in Africa—Kinshasa, Nairobi—the security is not as good in most cases. What are you trying to do to improve that?

Mr Darling: You are absolutely right that the system is only as good as the weakest link in it. It is one of the things I am concerned about, but it is not just the stereotypical airport you describe in areas where there may be a lack of awareness, there are other countries in different parts of the world which ought to be aware of the problem and ought to be doing more than they actually do. Part of it is inter-governmental pressure, partly it is at departmental level and also the European Union itself is trying to drive up standards, but it is a matter of concern.

Ms Tompkinson: You are absolutely right to flag this up, it is one of the areas of greatest concern to us and we put a lot of effort into trying to tackle it. It is a difficult area for the reasons you have said, any airport can be the weakest link As I mentioned in my opening statement, we now have a number of people based overseas to work with host countries and to work through the Foreign Office. The Foreign Office also have in every post overseas an individual whose designated post is aviation security officer, so wherever you have a UK embassy or high commission there is someone in there with some aviation security responsibility although it will not be their whole job. In addition, we have a small number of people who are there full-time, they are aviation security experts, they have been trained in Transec and posted overseas to work with the host countries in their region to advise them about better standards of security. That is something we have to do through negotiation, host states have responsibilities for following international regulations, standards set by ICAO or the European Commission in Europe. We feel we can add value by working very closely with countries to advise them on how they could do better and, if need be, make some additional resources available to them. One of the things we do routinely is invite the officials from those countries to visit the UK to see how we do security at our airports so they can learn from that and we can talk to them on that. We also have one person whose full-time job it is to look to see where the Government could make some modest investment, through a fund available in the Foreign Office to practical projects overseas. So if a country cannot get its security right because it has a lack of resources, equipment or training, then we can help them with that in a very practical way.

Q68 Chairman: Secretary of State, can I ask about your National Security Committees? Do you appoint the people who sit on them?

Mr Darling: We bring them together; the Department brings them together.

Q69 Chairman: Who appoints them?

Mr Darling: It is more of an invitation than an appointment.

Q70 Chairman: Could you tell us what they do and what things they look at?

Mr Darling: There is one for aviation, one for railways and one for maritime. It is a forum to enable them to discuss current issues, to discuss future developments. For example, in aviation they discuss things like—

Q71 Chairman: Do they make recommendations? Are they accountable to anybody?

Mr Darling: It is more of a forum where you can bring people together.

Q72 Chairman: Even fora occasionally produce results.

Mr Darling: These ones do. In fact we would not have them if they did not have some purpose because I can think of better ways of spending a couple of hours than endless discussions. They have proved to be pretty productive actually and they sometimes do result in things which otherwise would take months to agree.

Q73 Mr Leech: I wanted to pick up on the point about people working abroad in other countries. Is that just outside the EU? Anyone who has been on holiday to the Mediterranean would probably agree that some of the practices in some of our EU partner states are not as good as they could be.

Ms Tompkinson: We do not have anybody based within Europe. It is obviously very close to us so we can make visits to our European counterparts. We work very closely with the European Commission. They have their own programme of regulation, 23/20, on which of course the UK's national programme is based—or their programme is based on ours, it depends which way you look at it. So there should be the same baseline measures in place across all European countries and countries should be adhering to that. It is the responsibility of the European Commission if countries are in breach of the European regulations to tackle that.

Q74 Chairman: Secretary of State, you and your colleagues have been very good and helpful to us but I think there are a lot of questions we still have to ask and this is probably not the time. I know you have been travelling overnight and I think you have been holding up astonishingly well; you did not even drop off in the middle of anything the Chairman was asking you. Could I therefore ask you, before I let you go, if we can send you a series of questions about one or two other aspects and you could send us some notes?

Mr Darling: If you let us have the questions you would like further details on, we would be very happy to let you have that information.

Q75 Chairman: Thank you. This is the beginning of quite a big amount of work and we are grateful to you.

Mr Darling: You may want to come back on some specifics.

Chairman: I think it is quite possible we will want to do that. In the meantime we are very grateful to you, Ms Tompkinson and Mr Grubb.

Written evidence

APPENDIX 1

Memorandum submitted by Merseytravel

INTRODUCTION

1. Merseytravel is the operating name of Merseyside Passenger Transport Authority (MPTA) and the Merseyside Passenger Transport Executive (MPTE).

2. The PTA is comprised of 18 elected councillors drawn from the five metropolitan district councils on Merseyside: Liverpool City Council, Sefton Metropolitan Borough Council, Knowsley Metropolitan Borough Council, St Helens Metropolitan Borough Council and Wirral Metropolitan Borough Council. The PTA was established in 1986 on the abolition of Merseyside County Council.

3. The PTA sets the transport policies in the sub region, and the PTE implements those policies. These policies are described in detail in the Merseyside Local Transport Plan, a statutory document covering the period 2000–01 to 2005–06. The provisional Local Transport Plan 2 was recently submitted to the Department for Transport and will be finalised soon which will set out the transport priorities for the sub region between 2006–07 and 2010–11.

4. Whilst there are currently seven PTA's and PTE's in the metropolitan areas in the UK, Merseytravel is unique in that the PTA and PTE is one operating organisation.

CONTENT

5. There are over 160 million journeys per year on the Merseyside bus network, over 33 million journeys per year on the Rail network and approximately 750,000 journeys per year on the Mersey Ferries. The Mersey Tunnels allow over 30 million vehicles per year to pass through their portals. Overall the majority of transport journeys pass without incident, however those journeys which do encounter problems often attract a disproportionate press.

6. Merseytravel's aim is to create a single integrated public transport network which is accessible to everyone. An important element of the transport journey from passengers or intending passengers is the perception of transport security on the network. Merseytravel has invested significant time and resources to help reassure the travelling public that the network is safe. These interventions have been implemented by a number of mechanisms as detailed below.

TRAVELSAFE BOARD

7. No one organisation has the necessary skills, breadth of influence or resources to ensure the transport network appears to be safe; so Merseytravel has established and chairs the TravelSafe Board. The Board has representatives from the following organisations as follows:
— All 5 districts Crime and Disorder partnerships.
— The CPS.
— The Merseyside Probation Service.
— Merseyside Police.
— BTP.
— The PTA.
— The local bus operators.
— The local rail operators.
— Network Rail.
— Local District Partnerships.
— Go-NW.
— Mersey Ferries.
— Mersey Tunnels.
— The Taxi trade.

The Board has produced a strategy and is intelligence-led to ensure the joint resources of the above agencies and organisations are brought to bear in a co-ordinated manner.

8. Merseytravel has invested significant sums in providing grants to bus operators to install CCTV systems on buses to evidential standards. Similarly, the recent re-furbishment of the Merseyrail Electrics Train fleet has included the installation of CCTV to all the carriages. Also the number of CCTV cameras to rail and bus stations has been increased and improved. Bus Station security has been independently reviewed by Crime Concern and the recommendation of their audits has resulted in an improved waiting environment.

9. Merseytravel is an active member of the "City Safe" partnership and has provided accommodation space for a joint Liverpool Control Room which is the focal point for CCTV in the City. This it has done as part of a three-way Partnership with Liverpool City Council and Merseyside Police.

10. In order to make the best use of available data Merseytravel has employed a specialist member of staff to co-ordinate intelligence to produce reports on incidents, using information supplied by transport operators, etc. This is called the "IRIS" system and is used to better direct partnership efforts on "hotspots" identified. There is an argument for introducing a consistent reporting system across the UK.

Policing

11. Merseytravel have established strong partnerships with Merseyside Police and BTP. This has included a Merseyside Police Sergeant and a British Transport Police Inspector both of whom have been on secondment. This has further strengthened the inter-relationship between policing and TravelSafe, allowing cross-fertilisation of ideas between the various organisations. We have provided funding for 12 CSOs on the bus network and six CSOs on the rail network (the first of these in the UK). Indeed arising from this initial commitment, BTP have recently announced that they would place additional CSOs on Merseyside, funded from their own budget.

12. Merseytravel has built up excellent relationships with Merseyside Police and BTP and has embedded officers from both forces working alongside Merseytravel staff. This is very valuable and allows considerable partnership progress to be made on joint initiatives to reduce crime and progress a safe transport network.

13. Representatives from Merseyside Police and BTP attend some of the regular meetings organised by Merseytravel.

TravelSafe Officers

14. Merseytravel employs dedicated TravelSafe officers and commits significant budgets to the progression of this policy area. We are active members of the STOP (Safer Travel on Buses and Coach Panel) and in the past Merseytravel have organised a conference to promote TravelSafe and share experiences to move the agenda forward.

25 October 2005

APPENDIX 2

Memorandum submitted by the National Union of Rail, Maritime and Transport Workers

Issues Arising from the London Bombings

The National Union of Rail, Maritime and Transport Workers (RMT) welcomes the decision of the Home Affairs Committee to hold an evidence session on the "issues arising from the London Bombings".

RMT sends our condolences to the families of those people tragically murdered as a result of the bombings on 7 July. Our members were on hand in the immediate aftermath of the terrorist atrocities at Kings Cross, Russell Square, Liverpool Street and Edgware Road to provide comfort and support to those passengers who were injured, to evacuate stations and to de-train passengers caught up in the bombings. RMT members also assisted members of the travelling public on 21 July after the thankfully unsuccessful terrorist attacks and in addition were working at Stockwell station on 22 July when Jean Charles De Menezes was shot dead.

The appalling events in July self-evidently raise a series of important questions in relation to the safe and secure operation of the London Underground. Since the attacks RMT has held a number of useful meetings with the Mayor of London where substantial agreement has been reached in relation to train radios and staff numbers across the network. Progress has also been made in relation to the Fire Precautions (Sub-Surface Railway Stations) Regulations 1989 and discussions are also continuing with the ODPM on this matter. We would nevertheless hope that the issues which we will raise in our note assist the Committee during the course of its deliberations.

THE HIDDEN OBVIOUS AND TYPICAL (HOT) PROCEDURE

The HOT procedure is used by LU staff to determine whether packages and parcels left on the underground present a danger to network operations. RMT believes that following the terrorist attacks the procedure should be robustly and rigorously applied to ensure the safe operation of the network and protect the interests of the travelling public. It should not be used, as some RMT representatives have reported to us, primarily as a means to identify lost property.

We believe that the HOT procedure should be applied in such a way as to ensure that the service is suspended if an unattended item is within the line of sight of any running line. In addition where security checks are carried out on the seat tags in the passenger carriages and the tags are found to be broken the train should not be put into service. Staff should also be encouraged to take a robust attitude to packages left on station platforms and in booking hall areas, with full evacuations of stations taking place if staff believe that items are suspicious and therefore potentially dangerous. During the course of recent discussions the Mayor agreed that he would review the application of the HOT procedures.

TRAIN RADIOS

The July terrorist attacks highlight the need for an efficient train radio system which enables the driver to be in constant contact with the Line Controller. It is essential that in the event of an incident or emergency a communication system is in place which stops the driver from proceeding towards a dangerous part of the network and enables him/her to de-train passengers at an appropriate safe and secure location. Regrettably train radios all too often fail. Transport for London's 2005 report into the second year of the PPP describes the Connect PFI train radio replacement project thus;

In the last year both the Northern and Piccadilly lines have suffered severe disruptions caused by the failure of life expired train radio systems. It is therefore crucial that the new system is delivered. This was originally due in October 2003. The programme is now running over budget and four years late. Despite progress in the last year which saw enabling works (to provide space and power for the new equipment) reach 82% of completion and the radio system reach 60% of completion, performance by the contractor is not good enough and there have been changes in personnel and approach to expedite delivery.

RMT is concerned that the train radio system remains inadequate. We believe that for reasons of safety a "no radio no train" policy should be introduced by LUL and that works should be undertaken as a matter of the highest urgency to complete the introduction of the replacement radio system. During the course of recent discussions the Mayor agreed that trains should not be put into service with defective radios.

STAFF NUMBERS

LU staff played an essential role in the immediate aftermath of the 7 July bombings. We believe that commitments should be made by LU management not to reduce staff numbers across the combine. This will ensure that in the event of future attacks sufficient visible, well-trained staff are on hand to assist passengers who might be trapped on trains and to safely and efficiently evacuate stations. During the course of recent discussions the Mayor agreed that there should not be any future overall reduction in staff numbers.

GUARDS

The Committee will be aware that ridership on the London Underground fell significantly after 7 July. Thankfully passenger numbers are now beginning to climb again. RMT believes that the travelling public should have confidence that their journey will be safe and secure. We believe that visible, well-trained staff should be present to provide information to the travelling public and to offer assistance and support in the event of an incident or emergency. We are therefore of the view that LU should begin the process of re-introducing guards across the underground network.

Whilst fully aware that guards are unable to stop terrorist or suicide bombers they can help passengers to de-train as safely as possible in the event of an emergency by for example ensuring that they do not evacuate onto potentially live rails. This is particularly important in the event of the driver being injured or otherwise incapacitated.

At Shepherd's Bush on 21 July the second trained member of staff on the train, who on that particular occasion was travelling in the drivers' cab, was able to go through the train to re-assure passengers whilst the driver was trying to communicate with the Line Controller.

BREATHING APPARATUS AND DRIVER CAB BULKHEADS

RMT believes that research should be commissioned to investigate whether the introduction of breathing apparatus for operational staff and measures to strengthen driver cab bulkheads would increase safety and security in the event of future terrorist attacks. During the course of recent discussions the Mayor has agreed to examine our representations on this matter.

Fire Precautions (Sub-Surface) Regulations 1989

The Fire Precautions (Sub-Surface) Regulations 1989 were introduced following the Fennell report into the November 1987 Kings Cross fire disaster in which 31 people died. The regulations include wide-ranging fire fighting and precaution measures, including means of escape, means of fighting fire, minimum staffing levels and staff instruction/training, means of detecting fire/warning of fire and fire resistance.

In 2004 the Office of the Deputy Prime Minister (ODPM) proposed to replace the regulations as part of the Regulatory Reform (Fire Safety) Order 2004. Following representations the House of Commons Regulatory Reform Committee recommended that the regulations should be retained. The ODPM agreed to accept the recommendation until such time as guidance to replace the regulations had been drafted.

The current position is that the ODPM wants to repeal the regulations by February 2006 if they remain convinced that the 2004 Fire Safety Order and new guidance does not decrease safety on London Underground and the mainline stations to which the regulations apply.

Despite this assurance RMT believes that the July events make the protections contained in the provisions of the 1989 regulations all the more essential. We remain concerned that the proposed 2004 Fire Order reverses the burden of proof in relation to the fire safety regime in force on the London Underground.

Currently London Underground Limited has to satisfy the fire authority that a specific minimum standard at a particular location is inappropriate, unnecessary or not reasonably practicable. However the approach adopted by the 2004 Regulatory Reform Order reverses this arrangement meaning that in the future it would be for the fire authority to show that the employer has failed to carry out a suitable and sufficient risk assessment.

In fact minimum standards apply to many other hazardous situations. Indeed Article 24 of the new Regulatory Reform Order recognises the need for them in response to serious fire hazards.

Despite the claims that the current regime is overly prescriptive RMT believes that the 1989 Regulations do offer sufficient flexibility.

The current arrangements allow for modifications to be made to the 1989 regulations if the employer can satisfy the fire authority that a minimum standard at a particular location is inappropriate, unnecessary or not reasonably practical. Current legislation already requires a risk assessment to be carried out in order to cater for the widely varying characteristics found in each workplace. The 1989 Regulations merely prescribe minimum standards upon which the findings of such an assessment should be built. These minimum requirements are not blunt instruments that impose disproportionate requirements upon the rail industry. It provides for some flexibility in that the fire authority can grant an exemption from many of the requirements where they can be shown to be inappropriate, unnecessary or not reasonably practicable.

RMT believes that the ODPM should uphold the necessary protections provided by the Fire Precautions (Sub-Surface Railway Stations) Regulations 1989 and therefore keep the regulations on the statute book. We believe that in light of the terrorist attacks any attempt to remove the Regulations would disregard the public's concern for safety and security on the underground and mainline networks.

RMT thanks the Committee for taking the time to read our note and hopes that the issues we have raised are useful to members during the course of their deliberations.

APPENDIX 3

Memorandum submitted by the Road Haulage Association Ltd

Introduction

The Road Haulage Association (RHA) was formed in 1945 to look after the interests of haulage contractors in various areas of the country, in effect, amalgamating local organisations that had already been established. The Association has subsequently developed to become the primary trade association representing the hire-or-reward sector of the road transport industry. There are now some 10,000 companies in membership varying from major companies with over 5,000 vehicles down to single vehicle owner-drivers.

Background to the Industry

The road haulage industry plays a pivotal role in the UK economy carrying over 80% of all domestic freight. In 2003 this amounted to:

— 1,053 million tonnes carried by hire-or-reward vehicles;

— 590 millions tonnes carried by own-account operators" vehicles;

— a total of 1,643 million tonnes of goods transported by road;

— 152 billion tonne kilometres on road transport;

— an average length of haul of 46 kilometres for rigid vehicles, 133 kilometres for articulated vehicles and 92 kilometres as an overall average.

There are approximately 52,000 businesses in the industry and between them they operate some 430,000 vehicles over 3.5 tonnes gross vehicle weight.

GENERAL COMMENTS

Security is a major concern to both the road haulage industry and also to its customer base. In recent years we have experienced a significant increase in the theft of vehicles and/or loads by professional criminals engaged in organised crime. Although the absence of any consistent approach to data collection makes it difficult to quantify how much road freight crime costs the United Kingdom each year, thefts recorded by Truck-Pol[1] amounted to approximately £74 million in 2003/4 and had a detrimental impact on over 3,500 jobs. This is a conservative estimate, as over 55% of crime reports received by Truck-Pol do not specify the load value. In addition to the value of stolen loads millions of pounds worth of tax is lost to the Treasury each year.

SPECIFIC TRANSPORT SECURITY ISSUES

1. *Terrorist threat*

Recognising that the UK road freight sector may be a possible target for terrorism, post 9/11, the Road Haulage Association is involved in proposals to enhance and develop the existing industry/police Truckwatch[2] scheme. The aim is to ensure that a commercial vehicle and/or its cargo will not be used as a weapon, or to facilitate the delivery of such a weapon. The objective is to raise awareness of the true level of terrorist threat in a controlled manner, by gathering information and reporting to the appropriate authorities any intelligence that is likely to be of benefit to government enforcement and intelligence agencies in the fight against crime and terrorism, and to reduce the vulnerability of the road freight sector to criminality and terrorist attack, as well as any other security/criminal incident. A request has been formally submitted to the Police Information Technology Organisation (PITO) to provide an automated facility to notify Truckwatch within minutes of a stolen report being placed on the Police National Computer (PNC), but this has not yet happened and together with the lack of funding for a project manager the scheme has presently stalled.

2. *I.D Cards*

Drivers arriving and departing from ports of entry are not presently checked to establish their identity. The checks on identity relate solely to vehicles, container numbers and the pin number (if the port employs that method). Most ports operating pin number collections do not have an interface with the driver, all transactions being completed by electronic means, albeit the driver is being monitored and recorded on CCTV. It is therefore impossible for the HGV driver's driving licence to be used (for identity checks), as there is no person available in the release and arrival process to check against the photograph of the driver. What we believe is required is a quality method of identifying a driver visiting a port, whether delivering or collecting a container and leaving an audit trail that is difficult to circumvent. An Entitlement Card with a bio-metric facility incorporated into the card issued to the driver and a reader facility at the port could provide an economic solution, but if the industry is to accept this then a single card would need to be accepted by all ports and other secure establishments.

3. *Driver Security*

The security problems facing road freight transport go beyond the physical. Commercial vehicle drivers are also affected by problems of lone working. A driver's truck cab is his office and it is a legal requirement for employers to address commercial vehicle driver safety in that workplace. Lone workers should not be more at risk than other employees and, in the event that a worker suffers an injury or mental and emotional distress through the lack of provision of reasonable safety and security measures, the employer may be held liable for damages in law.

Employees in professions traditionally thought of as at risk are generally afforded excellent means of protection. Specialist security van drivers for cash collection companies, for example, are issued with protective clothing and reinforced windows and doors. However, observers point to the lack of safety

---

[1] Truckpol is a small team of police officers operating under the umbrella of the Metropolitan Police Stolen Vehicle Squad that collates and disseminates offences and intelligence regarding HGV crime, funded entirely outside the force budget by the insurance and haulage industries including the Road Haulage Association and matched pound for pound by a Home Office grant.

[2] Truckwatch is a voluntary and independently sponsored crime prevention initiative run jointly by the Road Haulage Association, the Freight Transport Association and presently operated through six of the forty three Police authorities within England and Wales.

provisions for general truck drivers who can unwittingly assume the role of unpaid security guards. By the very nature of their job, they are isolated and largely unprotected—sitting targets for criminals when parked in secluded lay-bys or insecure and poorly lit truck stops (see section 4 below).

Hijacks and attempted hijacks increased dramatically in 2004, averaging seven per month and peaking at 15 in November of that year. The level of violence also appears to be on the increase, with drivers being assaulted and threatened with iron bars, hammers, knives and firearms. The propensity of hijackers to abduct the driver or security guard and detain them for several hours to facilitate the theft also appears to be increasing.

4. *Truck Parking*

The current provision for lorry parking is declining as many local authorities redevelop existing facilities for more "profitable" purposes, such as housing and commercial development. The problems currently being experienced are inhibiting the efficient carriage of goods and increasing the risk of these drivers being involved in an accident. The lack of secure facilities also means that drivers and their loads are also at greater risk of crime, as high value loads have often to be parked at the roadside or in other unsuitable locations.

Although as a nation we are dependent on road transport for moving goods and people around, there are no published standards or guidance on what a truckstop facility should comprise of, or what standards should be adopted for factors such as size, layout, construction etc. The Road Haulage Association would like to see government produce a Planning Policy Guidance Note to assist planners on the need to provide facilities to enable this vital activity. With the introduction of the Road Transport (WTD) Regulations from 4 April 2005, as well as the anticipated changes in driving hours regulations, the need for appropriate truck parking facilities is only going to increase.

5. *Smuggling*

Another problem faced by the employers of vocational commercial goods vehicle drivers is the constraints of the Data Protection and Rehabilitation of Offenders Acts, with regard to the ability to be able to carry out sufficient investigations into a prospective employee's background before deciding whether that person is of a satisfactory level of trustworthiness to be allocated to a vehicle that may well have a value in excess of £100,000 and could also be used for nefarious activities without the owner's knowledge.

Although an employer may have carried out all checks that are presently accepted and available before taking on new staff there is still the possibility that someone employed as a long distance lorry driver may carry out activities whilst out on the road (eg smuggling) that lead to a company vehicle being impounded and proceedings being taken against the employer, with little likelihood of mitigating circumstances being taken into account.

Following discussions with HMRC, the RHA provides advice to its members on measures they should take to protect themselves from the illegal actions of employees and to prove to enforcement authorities that all reasonable steps have been taken. However, until employers are able to conduct more through checks on potential employees, these problems will continue to arise.

6. *EU Customs Code*

With regard to security amendments to the Community Customs Code (Rev 1 to European Council Regulation 2913/92 (TAXUD/1250/2005)), which is the subject of a consultation process and covers trade across EU borders, Customs will be able to offer operators the status of Authorised Economic Operator (AEO), subject to the production of satisfactory legal and solvency requirements, in three parts: simplified procedures (1), security (2) or a combined recognition (3). However, although the terms of the amendment are as yet undefined, we believe that the proofs required would largely be those already made available by operators when applying for a Commercial Goods Vehicle Operator Licence. Therefore, we are unsure as to what the benefits of this initiative would be, especially taking into account the inevitable additional costs involved.

Although the scheme is voluntary, but not free for the operator to administer, it is not clear why anyone should want AEO status unless penalties are to be introduced for those who do not take it up. There is the concern that, in the long run, AEO status will become mandatory for all operators trading across EU borders, thus reducing trade facilitation, competitiveness and the Lisbon Agenda.

7. *Information on Freight Movements*

The Home Office has recently started a consultation regarding Police access to information on all freight movements, both inside the United Kingdom and presumably across the EU. The only way for such access to be effective in a risk based security regime is for the Police to receive notification of movements from shippers and/or hauliers in advance, rather as Customs intends with the Customs Code. However, the

cost/manpower implications of this have not, to our knowledge, been calculated. Put together with the Customs Code amendments, both would seem to have an adverse effect on EU trade and place significant additional burdens on the haulage industry.

8. *The Wider Cost of Crime*

The road freight sector suffers heavily from crime, which can have a crippling affect on business. This includes increased insurance premiums; the cost of buying and/or hiring replacement vehicles; failure to meet customer orders; loss of revenue; stress on management and staff, sometimes involving crimes of violence even redundancies and loss of business. Lorry and load theft is never a victimless crime. Customers suffer and so in turn does industry in general when these customers are lost. Insurance premiums are based on claims experience. Whatever is paid out in one year will be the basis for premiums for the following year and so it goes on. There is a compelling economic need for clearer public awareness of the true cost of this type of crime and its links with other criminal activity.

Road freight theft has become a highly profitable criminal enterprise with an average loss per incident of £32,125. This has a significant impact on the UK economy, through direct and indirect costs to business, as well as the effect on the way the UK is perceived by multinational companies and by supplying the grey economy with a ready supply of stolen goods. The criminal profits can then be used to fund further serious and organised crime.

Road freight crime needs to be moved up the political agenda. Until lorry crime becomes a KPI for the relevant authorities it is unlikely that the situation will improve. The National Criminal Intelligence Service has been charged with producing a "Baseline Assessment" for the Association of Chief Police Officers on the subject of HGV and load theft.

It could only be a positive step for the Home Office to recognise this type of crime as a specific offence, which is quite distinct from the existing definition of "Theft of or from a motor vehicle."

At present there is not a separate definition/code available whereby the relevant authorities can record the involvement of "organised crime" in commercial vehicle/load theft. The Home Office has the ability to introduce a tick box on the crime recording form for any offence that they believe warrants attention. The addition of a new tick box would give an immediate indication as to the size of reported organised crime in the UK.

CONCLUSION

In Britain today policing has become largely localised, with autonomy and local objectives playing little part in the wider picture. Currently resources do not exist for dealing with middle of the road organised crime—too big for local command units and too small for the National Crime Squad. There is one exception in the UK haulage industry and that is Truck-Pol.

At present Transport Security is dealt with by various departments and given varying degrees of importance. For this issue to be addressed effectively, co-ordination and information sharing between Government departments must be improved.

October 2005

APPENDIX 4

Memorandum submitted by British Airways plc

1. INTRODUCTION

1.1 British Airways welcomes the opportunity to submit evidence to the Transport Select Committee on the subject of transport security.

1.2 The airline's main base is London Heathrow Airport, the UK's primary international hub airport and one of the busiest airports in the world. British Airways also operates from 11 other airports in the UK, and worldwide, to 153 destinations in 70 countries. Its franchise partners take the airline's colours to an additional 85 destinations in a further 17 countries.

1.3 Security and safety are of the utmost importance to British Airways and at the core of all operational decisions. Annually, the airline spends more than £120 million on security across its network.

1.4 Following the tragic events of September 11 2001, British Airways spent £100 million on upgrading cockpit doors and the installation of CCTV on its fleet of Boeing and Airbus aircraft.

2. Overview

2.1 The UK has been at the forefront of security regulation and technology in the post-Lockerbie security environment. Measures such as hold baggage screening systems were implemented in the UK many years ago at significant cost to the UK aviation industry. These are now being introduced by other countries, currently Italy and Canada, although they are being funded by their respective governments.

2.2 The level of threat to civil aviation in the United Kingdom is assessed as "substantial". This level is a judgement applied by the Government's security services, and sits outside the control or influence of airlines. The translation of threat into measures to protect aviation against terrorism is the responsibility of the Department for Transport's TRANSEC team.

2.3 The regulations that govern aviation security measures for UK airlines and airports are determined through both EU legislation and legally enforceable Directions issued by the UK Department for Transport (DfT).

2.4 The DfT's Directions represent a significant increase in regulation over and above the EU requirement. This raises the issues of whether the UK provisions represent proportionate and reasonable regulation relative to EU standards, and whether the mechanism for determining regulatory fairness is adequate.

2.5 British Airways believes there is over-regulation in the UK when compared with security regimes existing in both Europe and the US in particular. This compromises the competitive position of the United Kingdom's airlines and airports.

3. General Principles in Europe

3.1 By definition, international airlines operate across national boundaries and compete with a large number of other carriers from around the world. Every country has its own approach to security and decides on the extent of aviation security measures to be employed, based on threat, historical precedent and political imperatives.

3.2 Within Europe, the European Commission has implemented common standards across airports and airlines, governed by applicable EU legislation, in an attempt to ensure a satisfactory platform for aviation security measures and to ensure the consistency of measures applied. This has raised the standard of security within the EU to what is widely accepted as a sound "baseline" level for aviation security measures for most of the 25 Member States.

4. General UK Position

4.1 In the UK there are more than 50 additional measures required by the Department for Transport and Government to be implemented by UK airlines alone, over and above those stipulated within EU Regulation (the European "baseline"). There are further requirements for airport operators.

4.2 These additional regulations are required to address the prevailing threat against UK aviation interests. It is contended that the threat in the UK is higher than that prevailing elsewhere in Europe and as a result, further measures must be applied. The industry acknowledges this viewpoint, but believes the threat is higher as a result of the UK's higher anti-terrorism profile, a function of Government policy.

4.3 To British Airways' knowledge, no Regulatory Impact Assessment (RIA) has ever been undertaken to demonstrate that the additional requirements are either proportionate or reasonable to address the assessed threat. If such an assessment has been undertaken, its analysis and conclusions have not been shared with industry, nor was it consulted.

4.4 We believe this runs contrary to the Government's stated intent to implement regulation that is both fair and reasonable and does not overtly disadvantage UK businesses. As far as the industry is able to determine, the Department for Transport has no financial accountability for the additional cost burden it places on Industry through the imposition of additional measures.

5. Impact on UK Aviation

5.1 The additional measures are very much in excess of what the rest of the European airline industry recognises as "baseline" and currently cost British Airways alone approximately £10 million per annum.

5.2 There are three consequences of these extra requirements. The cost of implementing these measures is of great concern, as indicated above. There are also operational and customer service implications as a result of the complex implementation of them. Finally, UK airports and airlines are placed at a competitive disadvantage *vis-à-vis* non-UK airports and carriers.

5.3 Some of the measures, for example passenger segregation, constitute an operational impediment that cannot be reversed once introduced, due to the physical and structural infrastructure changes required.

5.4 At a European level, the costs and complex implementation of the measures required in the UK reduces the competitiveness of British international carriers and airports compared with the major European players such as Air France and Paris CDG, Lufthansa and Frankfurt and KLM at Amsterdam.

6. SPECIFIC EXAMPLE

6.1 Certain aspects of UK policy, for example the segregation of all transferring passengers from others, indicate that the Government's base assumption must be that the security screening processes applied to passengers originating within Europe must be suspect and cannot be accepted as sufficiently thorough for transit within airside areas of UK terminals.

6.2 Apart from the UK, no other EU country requires passengers previously screened in another EU state to be re-screened again before boarding their aircraft. Segregation is not required for transfers between flights operating within the EU.

6.3 UK airports and airlines are required to segregate all arriving passengers and re-screen them, regardless of the thoroughness of the process applied to the customers at their point of origin. This also ignores the fact that they have just completed a flown segment into the UK, probably on a UK-registered carrier.

6.4 The inference is that all arriving passengers are "unsafe". The logical extension of this is that all arriving flights are "unsafe", despite being accepted as safe to fly to the UK. Segregation and re-screening of passengers has the highest impact in terms of cost and operational impact that competitors within Europe do not have to bear.

7. GENERAL PRINCIPLES IN THE UNITED STATES

7.1 In the United States, the security situation is even more distorted. The US Government has subsidised security infrastructure, in addition to the general and direct subsidies to many US carriers through compensation, loan guarantees and Chapter 11 bankruptcy protection.

7.2 The US Government in turn reclaims some of that expenditure through the fees imposed on airlines. These monies are collected from Non-US carriers as well as US airlines. The fees fund activities such as the deployment of "Sky Marshals", from which Non-US carriers gain no benefit, thus there is an element of overseas carriers funding the US subsidies.

7.3 The US also imposes additional measures to be implemented in the UK for flights to the US. These measures are imposed on carriers directly by the US Government and are not subject to agreement with the UK Government, despite the requirement to implement the measures at UK airports. All costs of such measures are borne by airline operators.

8. IMPACT ON UK AVIATION

8.1 The UK Department for Transport does not accept US baggage screening standards as satisfactory and requires baggage flown in from the US to be re-screened at the point of departure in the US. Hence, British Airways and other UK airlines must apply further baggage screening at airport of origin in the US, in accordance with DfT requirements, at the carriers' cost. Baggage is effectively screened twice using two types of screening technology.

8.2 Despite these additional measures, such baggage is still not considered acceptable by the DfT for onward connecting flights from or within the UK without being screened again. This disregards the fact that this baggage must have been screened to an acceptable standard to permit flight from the US, on a UK carrier, into a UK airport.

8.3 Paradoxically, the US authorities do not accept the UK DfT's screening standards, so all baggage arriving into the US from the UK, and connecting to other flights at US airports, has to be re-screened as well. The cost of this is borne by airlines.

8.4 Although there are examples of harmonisation of standards between the EU and US, for example aircraft certification, it does not seem possible to reach a reciprocal agreement on screening or security measures.

9. THE WAY FORWARD

9.1 British Airways' experience leads it to the opinion that the UK requires the highest standards of security anywhere in the world, with the exception of Israel. The higher level of threat faced by UK aviation can be attributed to Government policy. However, none of the additional security measures required of the industry have been funded by Government.

9.2 The airline recognises that it would challenging, if not impossible, to regain a level playing field in a global context. However, it believes that some relatively simple changes to the regulatory processes applied to aviation security could provide an element of financial accountability by the Regulator. This would have the effect of lessening the burden on industry and providing "value for money" regulation.

9.3 British Airways has proposed, with widespread industry support, that the measures contained within the European "baseline" regulations should be *industry funded*. Additional measures, imposed by individual countries as a result of an increased threat due to nationality, must be *government funded.*

9.4 Under the proposal, all routine legislation would be preceded by a Regulatory Impact Assessment (RIA), which would be reviewed after one year. All urgent security legislation could be implemented without a RIA, but must include a "sunset" clause, by which time an RIA should be completed in order to make the legislation permanent.

9.5 Whilst the above would not redress the imbalance within the EU, it provides a control mechanism that would offer transparency between the security value created and the cost. It would also reduce disparity with the rest of Europe.

10. Summary

10.1 British Airways believes efforts must be made to secure consistency and harmonisation of aviation security measures with major overseas partners is essential, especially with the USA. There must be a focus on ensuring the basics are correct and meeting the emerging threats and risks as appropriate, rather than concentrating on closing loopholes by means of expensive additional measures which lack effectiveness due to their complexity and lack of credibility.

10.2 In response to a question from Lord Faulkner of Worcester in the House of Lords, on Monday 10 October the Lord Davies of Oldham stated that "*. . . the Government recognise that there is additional funding related specifically to the issues of terrorism and the safety of passengers and staff, which necessitates an increased Government contribution. There has been a contribution over the past year, an increased one over the coming year, and a three-year projected increase of support for that necessary expenditure.*". The transport system to which Lord Davies was referring was, however, surface transport, not transport by air.

10.3 British Airways considers this to be iniquitous. Airlines and airports ultimately pay for all security infrastructure and protection costs for the air traveller. The cost of the police presence at all of the UK's major airports is borne by the industry. Only at non-designated airports, which tend to be the smaller, regional sites, does Government fund police coverage.

10.4 This may have been acceptable in years past but no longer. Given the nature and extent of the threat prevailing today, and the attendant costs of security provision, it is unusual that the UK airline and airport industry has to fund security measures to an extent not seen elsewhere in the world. The negative impact, both financially and competitively, is substantial and we urge the Government to reconsider this situation.

25 October 2005

APPENDIX 5

Memorandum sumbitted by the Cyclists Touring Club (CTC)

The CTC has since 1878 provided a voice for cyclists in shaping transport policy and provision, and today represents some 70,000 members and affiliates mostly based in the UK. The use of the bicycle as transport, and its value as a complementary mode to rail travel are key areas in which CTC and its members press for recognition and implementation of policy and projects

The bicycle delivers a number of key benefits in moving people in large numbers and to diverse destinations, and it has great use in this respect for bringing passengers—especially commuters to and from rail interchanges. It equally delivers at the level of individual trips, and has a local impact on a par with that of walking, with minimal demand on resources and infrastructure, and with immediate use of almost all available roads, tracks and paths, yet with a demand for services purchased and delivered locally.

Government policy on transport recognises the effectiveness of cycles and rail as an integrated transport package, and, given that there is no capacity to take bikes on commuter trains at peak times, the solutions of cycle parking and cycle hire are promoted. For the most part, to date, the emphasis has been on cycle parking, and a very basic need for those making regular commuting journeys is for robust security, for bikes which are left all day or overnight, and often all weekend at the same location.

Naturally the introduction of portable items, which belong to members of the public into a station area raises the issue of management to ensure that the potential for any security risk does not arise—measures such as requiring all bags to be kept with their "owner" deals with luggage, and similarly the management of vehicle parking and access, essential for the operation of any station, can be set up in ways to minimise risk, and ensure rapid checking in the event of any alert.

CTC has worked with Transec and BT Police over the years to promote good practice in the management of cycle parking, and the current guidance permits cycle parking of most kinds at all security-ranked categories of station, with various safeguards built in to the management of the facilities, and identification of the cycles and users in some circumstances.

However we seem continually to encounter the mis-interpretation of Transec guidance and the failure of some operators—or specific station or area management to manage elements of their station inventory—like the cycle parking—effectively.

As noted the cycle parked regularly for long periods in the same area of open parking stands is vulnerable to theft and vandal attack. Because most cyclists in this group are regular travelers, solutions such as secure parking lockers or restricted access compounds, are a popular solution, which we will give examples of later.

For the occasional or casual user, it is unlikely that they will want to register with a station as a regular user, and so management of open access parking, if this is separately provided from a secure facility equally requires a robust regime. Nature, as is often quoted, abhors a vacuum, and in the absence of properly installed and managed cycle parking cycles will be attached to any fixed object conveniently located for onward access to the station.

Fortunately, most station management has got past the crude "no bikes here" signs which gave no additional advice or even penalty for parking. (see notes on best practice).

Higher security is available from cycle lockers, and these can be managed effectively, and even remain in use when (as happened in Exeter) a Royal visit to the site took place—because users are registered and use monitored. Transec guidelines spell this out, and regimes such as that set up by GMPTE, endorsed by BT Police and Transec, hire out lockers on several important stations in the GMPTA area, including Stockport, Wigan, Bolton, and I believe Manchester Piccadilly. However the pattern of railway management's decision making when considering security, and directives from Transec, does not have a very good record, when it comes to cycle parking.

Example—Edinburgh Haymarket Station

Perhaps the first instance of a poor management interpretation and execution of a Transec directive, which lead to a serious engagement between CTC and Transec to get guidance set down and available for those planning cycle parking at stations.

Interpreting a Transec directive, a team went to Edinburgh's Haymarket Station with no advance notice, and removed two Glasdon BR64 racks, which were popular, and located on Platform 1 (the platform least used by passengers). Local station staff were not consulted about ownership of bikes, most of which were used by regular commuters. Cycles were removed from the racks and dumped in a pile—at least two were reported stolen, and the racks placed in the car park—with little change in any risk of a bike carrying a package, as the location was simply on the outside of the same wall—if anything a worse condition, as the previous location had regular surveillance from platform staff and passing passengers. The lack of sufficient parking at this station sees bikes locked to street furniture around the station entrance, and high demand for taking bikes on the trains

Example—Nottingham Station—Described in Detail by Pedals Submission

The cycle lockers in place to the south of Platform 6 at Nottingham Station were installed in 2001 by Central Trains with financial assistance from Nottingham City Council. Their arrival follows a long saga of cycle locker provision running since 1980 and failures which seem largely to link back to a station management which does not take note of advice offered by local cyclists on how best to manage the installation, and fails to find the resources to do this. The current lockers are not signed from the main station, and the access arrangements were poor, with the announcement that the locker operation would be suspended "for security reasons". The poor management extends to the cycle stands in the Porte Cochere where Pedals report vandalised stands and abandoned/wrecked cycles. This is surprising, given the management claim that the station has a high security rating—the excuse to suspend locker use.

We therefore call for much greater effort to deliver the needed cycle parking in a more consistent and robust way to meet both security requirements and government policy on sustainable and integrated transport, so that the term "Transec requirements" is not used as a pretext for inaction and incompetence of the station management. The term "Transport Security" should take account of the security of parked bikes (and other station users' vehicles), and preventing their theft and vandalism, not just security in terms of reducing the risk of terrorist bomb attacks.

Example Bikeaway Lockers

The manufacturer developed a two-stage locking system, where the user locks through an external hasp using their own padlock, but the hasp is mounted on a lockable shaft to which only the station management or security officers have a master key. Lockers can thus be inspected at any time using a restricted issue lock system, whilst providing for a variety of operating systems.

The manufacturer has additionally incorporated viewing holes in the sides and door, in consultation with Transec, and offers a management pack for a new user to set up locker rental with the new installation. Other manufacturers have followed suit but few to the comprehensive level which Bikeaway is offering.

EXAMPLE THE RISKS POSED BY CYCLES

Our research suggests that since 1939 there have been four bombs connected with parked or moving bicycles on the UK mainland. Two detonated and one had fatal consequences. In every case the explosive devices were not part of the bicycle, but in the loads being carried. This points to the main risk connected with parked cycles being luggage left on the bike.

Most cycle—based bombs are set off when the bike is moved, and thus the encouragement of cycle parking in formal areas delivers bikes which are unlikely to be pushed aside by passing traffic—that noted there is a need for places to lean a bicycle where tickets are sold and proper provision here will deal with the potential for nuisance, and safety problems of having a random placement of cycles, in a busy booking hall.

I can think of Ashford International, Doncaster, Edinburgh Haymarket, Nottingham, etc but also of the GMPTE work with BT Police and Transec for their Bicycle Locker Users Club (BLUC) which uses tagged bikes, and user details on record. Equally on the positive side we can note the work of manufacturers such as Broxap, Lock-it Safe, Cycleworks and Bikeaway with Transec to develop locker designs which can be inspected but also provide secure parking. (Haymarket saw the cycle parking removed arbitrarily without any notice, or consulting even the local station staff, and bikes dumped in a heap—at least two were stolen)

EXAMPLE—ABERDEEN

In Aberdeen the cycle parking was provided, under cover and convenient for access adjacent to the archway which was used by wheeled traffic—mainly to get in to the car park—on the area at the North end of the station. On the pretext of complying with security issues the cycle rack was removed and placed away from the main concourse behind the waste compactor unit—hardly a pleasant place and certainly not secure of convenient. Cars, which are not inspected, continue to park in the area, whilst cyclists use any available fixed objects, except for rail staff who lock bikes to the ticket barrier or to the stair railings in the stair well leading up to the main station offices. The need is emphasised by the signs at the BT Police office to stop cycles being locked to the rails set (U-hoops) outside the door to keep the area clear.

CYCLE PARKING—BEST PRACTICE SHOULD INCLUDE SECURITY MANAGEMENT

Formal cycle parking should, just as car parking, have clear conditions for use posted which, for open access cycle stands need to include the following:

1. A liability waiver.

2. Where security rankings are high there is a need to spell out the requirement to remove luggage or leave baskets and attached items empty and open.

3. A notice that abandoned bicycles (which have not moved for xx weeks)—and damaged bicycles will be removed, and dealt with by (a procedure—CTC recommends putting the bikes into the existing lost and found property system, which disposes of them after a set period).

4. A reminder of good practice in securing a bicycle, and where a more secure location is available, details of how to register, rent or otherwise use it are posted. If a registration scheme to identify bikes is in operation this can also be noted.

Note: A National system which delivers a common standard to register cycles parked at stations should be considered—to deliver a simple numbered label which can be affixed to the cycle, and allowing station staff to readily contact the owner, and embracing the scheme devised by GMPTE (BLUG) for locker hire.

One effective way of monitoring abandoned cycles is to attach a parcels label around the tyre, and this is naturally destroyed if the cycle being checked is used.

A higher level of security both against theft and damage to the cycles, and providing identification of the cycles parked, can be achieved by using lockers and secure compounds. To date the locker systems available have used mechanical locks, and the first company to engage with Transec on locker design (Bikeaway) delivered an innovative system where the station management can by-pass the user's lock and inspect the locker at any time. This design also includes perforated panels which align to provide a means of inspection with commonly used equipment, and ground clearance which allows ventilation without compromising the security. Cycle locker schemes require a greater commitment to management than open cycle parking but can be managed on an area-wide basis, and possibly in the longer term, nationally.

The user "contract" should:

1. Require a regular renewal (research indicates that most people will pay a reasonable fee for a locker or other secure or valet parking).

2. A declaration that the user will use the facility solely for parking a bicycle and associated accessories.

3. A condition that the user is sole user of the locker or swipe card/key/PIN (for compound access).

4. A termination condition (failure to renew, breach of conditions of use etc).

5. A failure to provide condition (vandal attack, closure for works at station etc).

6. Record of the user and their contact details (ideally for the times when the cycle is parked).

The User contract can additionally:

7. Provide an opportunity to survey the clients, over a range of factors (socio-economic, cycling skills, common habits etc).

8. Offer added value to encourage regular users to register and use formal, managed parking (Third party insurance, special offers etc).

Notes: Open access, and coin in slot cycle lockers should be avoided in most situations as they are readily abused—storing contraband or providing mini-hotels for those living rough. Electronically controlled locks on secure rooms or compounds provide an audit trail on use, and experience with swipe/proximity card operation on a University site has kept cycle crime down to an almost insignificant level. Compounds with small groups of parking stands offer a diversity factor (more users than spaces) and high level of service (rapid access etc).

Where informally parked cycles cause an obstruction or other nuisance there should be two courses of action. The parked bikes suggest a demand for parking, and a convenient location, and the option of arranging formal parking at that location then takes the management back to (1) or (2). If there is a nearby formal location, or a formal parking arrangement cannot be put in at the location the signs which go up should cover the following points:

1. No bikes to be parked.

2. The nearest place for parking bikes.

3. The action taken against any bikes which are parked wrongly (noting that simply saying bikes will be removed without further information to enable its recovery is effectively saying "we are stealing your bike".

Conclusion

In conclusion, we call for a review of the remit of Transec to consider the relevance of management of security in a wider sense—both preventing terrorist incidents and the delivery of transport interchanges where the security of individuals and property is a naturally delivered result through planned measures which prevent rather than simply record unwelcome events for later action. We recognise that this will also require a careful defining of the roles of Transec and BT Police as specially skilled agencies to deal with security planning and management in the transport industry.

This should include the education, where necessary, of "station managers" in delivering a better result than currently seen at most transport interchanges to provide cycle parking in a more consistent and secure way. In doing this the management of parked cycles, as a detail of general security control should be approached as a scheme, which works to deliver the customer needs of convenience, and security in an intuitive way—so that the arriving cyclists naturally goes via the cycle parking area to enter the station by a direct and convenient route, and the station staff have where practicable a means to identify regular users, and manage the recognised risks associated with luggage attached to cycles, and use of enclosed storage, both of which can be operated with basic and simple measures, and in doing so deliver the Government's policy on sustainable and integrated transport.

In this way we hope that the use of the term "Transec requirements" is not played as an excuse for inaction and incompetence of the station management, and that Transec can offer a more active role in promoting managed secure cycle parking to a model of best practice, as highlighted in this submission, which aids their requirement to manage security risks.

APPENDIX 6

Memorandum submitted by the Freight Transport Association Ltd

Introduction

The Freight Transport Association (FTA) represents the freight transport interests of businesses throughout the UK. Its members range from small and medium size enterprises to multi-national public companies and are involved in all modes of transport. FTA members operate over 200,000 heavy goods vehicles, about half the UK fleet, are responsible for 90% of freight moved by rail and 70% of goods shipped by sea and air. This unique multi modal mandate enables FTA to speak authoritatively on all aspects of freight based on the broader transport needs of industry in the economy.

Following the 9/11 terrorist attacks industry became aware of just how vulnerable it was to the consequences of such events in the future. At the time actions to protect against terrorism were widely supported by industry. However, four years on a number of questions are being asked as to the proportionality of Government responses to the apparent threat, the costs to business and the lack of tangible benefits for those making the efforts to comply with new rules and guidelines.

FTA has been involved in transport security developments since the early 1990s, in the post-Lockerbie era. In the interests of its members, some 11,000 companies involved in freight transport either as operators or customers, FTA has tried to influence the shape of government security measures that benefit rather than hinder domestic and international trade.

This evidence considers domestic and international transport security issues and the issues of vehicle theft as well as linkages with the prevention of terrorism. We also consider future developments and how these can achieve maximum effect and the least disruption to freight movement.

SECURITY AND DOMESTIC FREIGHT MOVEMENT

(a) *The scale of the problem*

FTA conducted a survey of its members in 2003, the results showed that the estimated value of unrecovered losses of vehicles and loads was £160 million for van operators and £50 million for heavy goods vehicle operators. In total this represents losses of £210 million. However, this figure does not take account of consequential losses, in other words the cost of vehicle downtime or replacement, the administration required, the knock-on effects on customers and resultant increases in insurance costs.

In the period July to September 2005 the total value of heavy goods vehicles and loads reported stolen to TruckPol was £20.2 million. Undoubtedly the total is likely to be higher than this as not all truck crime is reported to the Police. Furthermore, not all police forces report into TruckPol.

(b) *Industry's role*

Industry has made significant strides forward in vehicle security in recent years. The Motor Insurance Repair Research Centre (MIRRC—Thatcham) has developed a 10 star rating system for truck security. The system is a scale indicating the theft difficulty level and mirrors the sort of scheme that has been in place for cars for a number of years.

Security on vehicles has also been improved. As well as an increase in the use of tracking devices there has also been an increase in the use of immobilisers on vehicles. The result of this is that there has been a rise in the number of drivers who are assaulted for their keys, which sometimes includes attacks using gas.

There are other areas where industry can focus its efforts in order to reduce thefts. These include anti-theft training of drivers and other staff and steps to make depots more secure as well as the purchase of more modern vehicles and technology to make theft more difficult. The vetting of drivers and sub-contractors is also important in reducing theft.

(c) *Government's role*

FTA believes that there is a greater need for a more joined-up co-ordinated approach between all the different Government, police and Driver and Vehicle Licensing Agency databases. This would allow more effective targeting of truck thieves and bring with it benefits in combating terrorism.

The way in which the police respond to truck crime also varies between different forces. This problem is exacerbated by the fact that forces do not have a shared understanding of what is a serious goods vehicle crime.

A study by the National Criminal Intelligence Service (NCIS) has concluded that a significant proportion of road freight crime is caused by highly organised criminal groups with their own networks across the UK. In FTA's view truck crime is serious because it has a significant impact on the UK economy. However, at present, due to the lack of effective policing, the financial rewards of road freight crime by far outweigh the associated risks of detection and prosecution.

The Government could put in place various measures to assist in reducing vehicle and load theft. Central to this in FTA's view is the need for provision of a network of secure HGV parking facilities or financial incentives for private parking operators to provide such facilities for goods vehicles. This would have a range of benefits including a reduction in thefts, the improvement of facilities for drivers and the removal of sources of nuisance from local residential areas.

Government could also assist through the provision of additional resources, via the Home Office, to support the development of schemes such as TruckPol and also to ensure that the development of SOCA (the Serious Organised Crime Agency) encompasses HGV crime as well as possibly providing anti-terrorist intelligence. At present, although there are a number of initiatives to combat truck crime, such as TruckPol,

Operation Indicate and Operation Grafton and others, these are hampered by a lack of Government funding. These initiatives are now all the more important because of the threat that stolen vehicles could be used in terrorist attacks, in particular those used to carry high consequence dangerous goods.

Dangerous Goods Security

The events of 9/11 focused attention on a new style of terrorism and as a result there was increased concern over the vulnerability of dangerous goods movements and the possibility that they could be used in an attack. Of special concern are high consequence dangerous goods, that is to say those that, if misused, can cause a large loss of life or seriously damage the economy or environment.

FTA has been closely involved in working with the Department for Transport's security directorate, TRANSEC, in the development of a United Kingdom voluntary scheme consisting of codes of practice and supporting guidance on road and rail transport security for dangerous goods. This has been done in advance of new UN security provisions being adopted in the ADR and RID international agreements which concern the carriage of dangerous goods by road and rail. A briefing note is included as an appendix to this submission and provides more information on this subject.[3]

In developing this voluntary approach FTA has been concerned to ensure that the measures used are practical for industry and that they are in proportion to the risks posed.

Security and International Freight Movement

In the 1990s FTA and other industry organisations worked with the UK Government to develop and implement a system of air cargo security that industry could tolerate and benefit from. This became known more popularly as the Known Shipper security regime.

The Known Shipper Security Concept

(a) *How it works in air freight*

Those downstream of the aircraft are responsible for securing and maintaining the security of export air freight. The benefit is simple, this is to prevent cost and delay from cargo screening that would otherwise be required at the airport before the plane flew. Nothing today flies without the airline having an assurance that cargo is known to be safe to fly, it is therefore said to be "Known Cargo". Policed by the security division within the Government's Department for Transport, shippers identify cargo for export by air, check it, pack it and keep it secure by limiting access to the cargo to authorised personnel only. They also check the vehicle loading and security measures for the road transit stage of the cargo's journey. These are the "Known Shippers".

Any receiving agent also needs to have security measures in place to protect the cargo from unauthorised access. They need to convince Government security inspectors that they can do this, and that they have also checked the security measures of their customers to make them known shippers and able to present "known" cargo. No screening is required if the known cargo remains secure. The agent, referred to as a "Registered Agent", maintains the security of the cargo in transit to the airline and it can be loaded straight onto an aircraft without screening.

The cooperation of all in the chain, and trust is essential for the system to work effectively. In this respect the regime was modified slightly following proposals coming from freight forwarders and shippers alike to ensure that known shippers are properly audited and vetted by independent third-party government authorised inspectors, rather than by the shippers' service provider, something which could have been open to abuse through commercial pressure.

(b) *Application to other modes and the supply chain*

In the post-9/11 world FTA was among the first to propose that the Known Shipper system be applied to all transport security in order to facilitate international trade and transport at the same time as securing it, and without over-burdening the companies involved.

Today, the Known Shipper approach to transport security has gained general acceptance in principle, although there is still some way to go to implement it around the world in a standard way. Importantly, the link between customs auditing regimes and security has also become widely accepted. This enables risk assessments to be made not just on the cargo, but looking at the origin, destination and route taken, the consignor and consignee and the nature of the business, in order to determine what cargo requires the specific attention of security personnel before allowing it to be imported or exported. The majority of freight, representing legitimate and secure trade, continues unhindered.

[3] Not printed.

The modal approach to transport security: high cost and unpopular

However, not all international security measures that have been introduced follow the Known Shipper approach. Rather than looking at the security of the freight itself from origin to destination, the focus was initially put on the security of ports, ships, aircraft and airports. Today all ports involved in international trade must comply with internationally agreed security put in place around the immediate vicinity of the ship and port. Clearly, the security of many ports and shipping lines must have been found seriously wanting as many claimed to face large extra costs almost overnight in order to comply with regulations designed to prevent unauthorised access to the terminals, ships and the cargoes.

The problem of cargo theft in and around ports is not a new one, and one might have expected that effective measures to prevent unauthorised access to cargo and cargo areas would have been something that the ports and shipping lines would have had in place anyway. Therefore it came as a surprise to many shippers to be asked by some ports and shipping lines to foot the bill. Shippers have been angered at the way security costs have been separated out from all the other costs of doing business, and in the case of port security charges, being imposed on shippers when they do not even have a commercial relationship with the ports.

The USA imposed a ruling in 2004 whereby ship-borne exports from Europe and elsewhere destined for the USA need to be known to the customs agency 24 hours before loading onto ships. It would be wrong to suggest that businesses have encountered difficulties complying with this requirement; nevertheless it should also be recognised by the US authorities and others (such as the European Union which is set to follow suit with its own pre-shipment notification) that this has resulted in increased lead times for many shippers which carries with it an inherent cost to industry.

FORTHCOMING DEVELOPMENTS

The European Union is soon to announce security proposals for all freight transport into and out of the territory of the EU and within the territory of the EU. Encouragingly, it looks likely to resemble an amalgamation of the Known Shipper concept (now becoming established in the EU air freight industry) with customs risk assessment procedures used to profile trade.

FTA is concerned to ensure that the various international approaches tie-up to form a single, co-ordinated and cohesive framework that is proportionate and practical. We also seek to make sure that the measures proposed are not confusing to those trying to implement them and that international and national trade is not adversely affected.

(a) *Keeping it voluntary*

FTA hopes that the steps to be proposed will be voluntary, and not made mandatory through regulation. In other words, industry, whether importers/exporters, manufacturers, retailers, distribution service providers, logistics companies, warehouse-keepers, or freight forwarders, may assess the costs and benefits to their businesses of compliance, and choose if, to what extent and how they need to comply.

Anti-terrorist security measures, comparable with theft prevention measures, require investment in systems, physical protection, personnel, training and planning. The extent to which one invests in these depends on an assessment of the risks. Risks vary from company to company, industry to industry, region to region and country to country and what is appropriate to one business may not be appropriate to another. Neither will companies know what the threat assessments are, as these are made by the security services based on their own intelligence and assessment criteria. Therefore companies will need to balance the level of security they adopt with what they believe will be the standards being sought by governments.

Governments will need to share with industry the types of measures and the minimum standards of security that will reduce the level of threat represented by industry and, thereby, the risk of having cargo delayed by the authorities for security reasons. Naturally, such measures and standards may vary according to the threat assessments being made, and industry will need to assess in turn how they respond.

PROVIDING INCENTIVES

The more incentives there are to invest in security the more companies will respond positively and enable the security services to better target the real threats and not detain legitimate trade.

FTA has long argued that security can yield some significant benefits to those that apply it:

— Prevention of delays at ports, airports and borders caused by security checks and cargo screening.

— Increased supply chain visibility exposing inefficient practices.

— Reduced theft.

— Brand protection through preventing a business being used by terrorists to deliver an attack—the impact of having one's name associated with such an event could seriously damage one's public image and wipe millions of dollars off the share price.

— Avoidance of security charges imposed by others in the supply chain on unknown cargo.

— Trade facilitation measures, such as reduced customs reporting or audit requirements.

(a) *Few tangible benefits apparent today*

The benefits identified above are difficult to value and may not be known until security measures have actually been implemented and company accounts examined.

For example, currently the number of reported delays caused by security controls to cargo, known or unknown, appears to be negligible. Therefore, avoidance of security-induced delays—one of the primary benefits cited for implementing cargo security, is not being realised. The realities of business mean that the majority of companies are not able to find the capital to invest, or seek the required authorisation for such investments, without being able to first demonstrate very tangible and real cost benefits.

(b) *What would represent an attractive and more immediate incentive to invest in improved security?*

There has been very little debate on this question, although FTA has attempted to raise this issue on numerous occasions with various governmental and international organisations.

FTA believes it is worth exploring the possibilities of reduced insurance premiums, caps on liability, tax benefits, reduced security charges where these are imposed by others, grants towards security systems, etc. All of these could have an immediate impact on a company's bottom line.

Failure to provide incentives may impede security

FTA believes that until the debate turns to provision of such benefits in a serious and meaningful way the groans of disapproval every time a new security initiative is mentioned will become louder and louder.

We also feel that governments need to take seriously the complaints of shippers about such things as security surcharges imposed on them by some sectors of the transport industry. FTA has repeatedly warned that the port and ship security surcharges are incompatible with the trend towards a known shipper security regime, as such non-negotiable charges fail to distinguish between secure cargo from secure sources and that which represents a greater security threat and which should legitimately be the focus of further security checks. The surcharges mean that there is less incentive to make the cargo known and less incentive to invest in security.

The drastic alternative would be to give industry no choice but to comply with security requirements and standards set by governments. However, this will leave industry needing to apply security measures that may potentially bear no relation to the actual threats they represent, or else result in cargo being unnecessarily delayed.

Questions are already being asked as to whether any of the security measures in freight transport are actually making a difference to the security of society and the economy. At present industry is only seeing the costs of security, and yet many in the transport sector suspect that there remain many loopholes through which terrorists and their weapons can slip and that there are many alternative, possibly easier, ways to bypass border security controls.

FTA believes that industry has mistakenly been thought of as a front-line defence against terrorism which it is not. We feel that too much focus is placed on industry to do the job of the security services and that the money being spent by industry on compliance would be better spent on increasing the resources of the security services.

Four years ago industry was fully prepared to co-operate in protecting against terrorist activities. Today, industry is increasingly questioning its role in combating terrorism and asking for evidence that it is even worthwhile, let alone cost effective.

This is a very serious development. If governments want industry to help then FTA members believe that they must be prepared to help industry. Too many governments, the UK Government included, expect industry to pay for security; yet it was not industry that attacked the Twin Towers in New York. So why, as more and more shippers are seeing it, is industry being treated as the wrong-doer and having to pay?

FTA believes that the time has come to redress the balance and that governments need to provide and pay for the incentives that will encourage industry to participate in the drive for more security for all our benefit rather than treating industry as both the defender against terrorism and, paradoxically, as the potential enemy within.

26 October 2005

APPENDIX 7

Memorandum submitted by Pedals (Nottingham Cycling Campaign)

EXPERIENCE WITH CYCLE LOCKERS AT NOTTINGHAM STATION

Introduction

The cycle lockers in place to the south of Platform 6 at Nottingham Station were installed in 2001 by Central Trains with financial assistance from Nottingham City Council. Although Pedals has been well aware of much pent-up demand for such a secure longer-term cycle parking facility, they have however suffered from a series of problems, particularly poor signing and poor management. The recent decision to suspend operation of the lockers, on security grounds, has just added one more problem to what was anyway a very unsatisfactory situation regarding cycle parking at this station.

It should be emphasised that the lack of managed and secure cycle parking is a serious problem—cycles in the Porte Cochere area at the front of the station are vandalised and the presence of apparently abandoned bikes and damaged stands for long periods shows that there is poor surveillance and concern from the station management. Faced with this situation many cyclists will make informal parking arrangements which will not be welcome at a location where good site management is a major element in providing robust security.

The saga of lockers and the station management's continuing failure to do anything positive in respect of the promotion and effective operation of these lockers and open access cycle stands seems surprising, given the supposed high risk status of Nottingham Station in Transec's rating scheme. Most high risk stations, we are aware, have clear signage and a management regime to warn against leaving luggage on cycles and to keep the cycle parking clear of damaged and abandoned bikes and damaged parking stands. Nottingham does not have such signs.

We are, furthermore, aware of other high ranked stations where, cycle lockers and parking are in place, and used in compliance with the Transec guidelines, but as the section below on the background history shows, the delivery of this much needed facility, which could be achieved, has been obstructed by the continuing obfuscation of the station management regimes at Nottingham station over the years.

We therefore call for much greater effort to deliver the needed cycle parking in a more consistent and robust way to meet both security requirements and government policy on sustainable and integrated transport, so that the term "Transec requirements" is not used as a pretext for inaction and incompetence of the station management. The term "transport security" should take account of the security of parked bikes (and other station users' vehicles), and preventing their theft and vandalism, not just security in terms of reducing the risk of terrorist bomb attacks.

Background History

The current lockers replaced two earlier well-used batches of cycle lockers installed at Nottingham Station. The first of these (three lockers) was installed on the southern side of the overbridge (between the concourse and the steps down to the platforms) by the then British Railways in the mid-1980s and were replaced a few years later by a circular block of eight wedge-shaped lockers. These were installed near the northern end of the same overbridge, also in a prominent position, and were also well-used. However, there were problems with the coin-operated mechanism and BR apparently found it difficult to get replacement parts. Another problem was that a new Station Manager became concerned about the possible danger to staff leaving the ticket office from possible assailants waiting behind the lockers. As a result of these problems the lockers were taken out of service by BR at the end of the 1980s, without any consultation, either with Nottinghamshire County Council (at that time the Local Highway Authority for Nottingham), who had paid for the installation of the lockers, or with Pedals who had campaigned for their installation.

A period of several years then followed in which Pedals tried to get either these lockers brought back into service, or new ones installed. In the early 1990s, following the installation of new luggage lockers, BR got the company responsible for managing these to agree to considering providing cycle lockers. However, the cost they proposed charging would have amounted to substantially more than the cost of parking a car at the station and the proposal therefore got nowhere.

The matter was left pending until an initiative by Nottingham City Council in the late 1980s, following their becoming a Unitary Authority in April 1998, and therefore taking over from the County Council responsibility for transport matters in Nottingham. The City Council indicated to Central Trains, who had by then taken over the main responsibility for managing Nottingham Station, that they would be prepared to subsidise the cost of new lockers. The discussions on these plans, in which Pedals was again involved, spent some time discussing the best location for these since by then concerns about security had grown. Pedals was again keen that the lockers should be as convenient as possible for users but Central Trains insisted that, for security and other operational reasons, the only practical at all convenient site that could be allocated was a bit to the south of Platform 6, on the south side of the Station.

In view of the decision to use this rather more out of the way site, Pedals emphasised the extra importance of good signing and other publicity to encourage usage of the lockers, as well as for hours of operation to be as long as possible (and including the length of time reasonably required by someone wanting to use them when away from Nottingham for a whole working day, and allowing time for travelling (outward and return journeys, eg to and from London). This was now all the more important because the previous lockers (coin-operated) had been available 24 hours round the clock.

With regard to signing Central Trains said that it was likely to take some time to provide permanent signs but they did agree meanwhile to provide temporary ones. However, even the provision of these has proved very problematic and, about four years later, the only sign to the lockers that has been provided is a small one adjoining the bay of Sheffield cycle stands in the Porte Cochere (forecourt) area informing users of those stands that "Cycle lockers are also available in this Station"! No other signs to show the lockers have ever been provided and it is Pedals impression that most station users therefore have no idea that they exist, let alone where they are to be found or how to use them!

When agreeing to the idea of temporary signs, as an initial step, Pedals emphasised that the only satisfactory permanent solution was to ensure that the directions to the lockers was included in future comprehensive signing. Many changes to the permanent signs were made, to prepare for the introduction of the NET Line One tram services in March 2004 (whose Station Street stop can be accessed from the mid-platform overbridge). However, despite Pedals many reminders about the need for signing, this opportunity to include references to the cycle lockers was not taken.

Fairly soon after the lockers were installed Nottingham City Council, in cooperation with Central Trains and Pedals, did issue a leaflet to publicise the lockers which had some impact but only limited because this was not followed up by proper signing within the Station. Pedals has helped to distribute copies of this leaflet.

A further problem discouraging usage was the difficulty that would-be users had in getting information on how to use the lockers. In theory information could be obtained from the information kiosk at the north end of the overbridge but in practice, feedback to Pedals suggested, the kiosk was often unmanned and, when it was, staff on duty often did not appear to know anything about the lockers let alone have the ability to give cyclists confident advice on how to use them. This was not very encouraging for people turning up, and wanting to leave their bikes easily, efficiently and quickly, and then catch their trains!

All these problems were pointed out on various occasions to Central Trains, including a meeting in July 2005 with Sharon Smith of Central Trains (Route Manager, Nottingham and Robin Hood) but still no action has been taken to improve the situation! The problems have also been raised on numerous occasions with Nottingham City Council staff responsible for liaising with Central Trains and for cycling, ie Richard Wood and Steve Brewer of City Development.

No attempt was made by Central Trains to learn from the experience of managing cycle lockers elsewhere, eg to reduce security risks by schemes that allowed the operator to keep an exact record of who was using them. After all this long saga of problems and a prolonged failure, after many attempts to resolve them, it was very disappointing recently to learn that the lockers had now, for security reasons, been taken out of service at the Station. This has been all the more disappointing when, we understand from the CTC Public Transport Campaigner, Dave Holladay, that not all cycle lockers at Category A stations have in face been taken out of service, in distinct contrast to the information from Central Trains that the decision for Nottingham Station was "non-negotiable while the current security rating was in position".

Since many local cyclists are reluctant to leave their bikes in the Porte Cochere area because of fears about theft and vandalism, the provision of more secure forms of cycle parking, especially for longer-term use, remains essential, and the present situation is most unsatisfactory. We would much welcome any help that the Committee's report can give, directly or indirectly, in getting these problems resolved.

FUTURE PLANS AT NOTTINGHAM STATION AFFECTING CYCLE PARKING DEMAND AND PROVISION

There are plans for a major redevelopment of Nottingham Station in the next few years and Pedals has made detailed comments about the importance of taking this opportunity both to improve and extend short- and longer-term cycle parking at the station and also to make further improvements in cycle access, to help reduce the need for station users to access the station by motor vehicle.

Cycle access has already improved with the series of measures in recent years by Nottingham City Council and British Waterways to improve the towpath of the Beeston and Nottingham canal which runs less than 100 metres north of the station, forming a very useful east-west traffic-free route to the south of the City Centre.

Overcoming the present security problems affecting the provision of good secure long-term bike parking will become even more vital in future once these major changes are implemented and the number of passengers using the Station grows even more rapidly than in the last few years.

October 2005

APPENDIX 8

Memorandum submitted by Virgin Atlantic

Virgin Atlantic is aware that the Transport Select Committee is currently conducting a short inquiry into transport security and will be taking oral evidence from the Secretary of State for Transport on Wednesday 2 November. Unfortunately, it has not been possible for us to compile a detailed memorandum in the time available. Nevertheless, transport security remains a very important issue to Virgin Atlantic and I thought it would be useful to send you a short letter outlining key areas of concern.

Virgin Atlantic takes its security responsibilities very seriously and has worked closely with the Department for Transport, Home Office and other agencies at the UK, EU and international levels as new security measures are developed and implemented. However, we have a number of concerns going forward:

— Lack of co-ordination across government departments: We remain concerned about the lack of co-ordination across government on security issues and would urge government, as a minimum, to expand the role of the Department for Transport's Transport Security Division (TRANSEC) to include responsibility for all initiatives relating to aviation security.

— Lack of cross-border co-ordination: Virgin Atlantic, along with other airlines, remains concerned at the role of the Safety Regulation Group of the UK Civil Aviation Authority in relation to the European Air Safety Authority (EASA). There is already considerable duplication between the powers and responsibilities of SAG and EASA. Terrorism does not respect borders—there is an urgent need for national authorities to co-ordinate with international organisations to work effectively together to establish global standards of airline security.

— Burden of costs: It should be borne in mind that terrorist action is aimed at governments and not the airline industry. Virgin Atlantic, in common with other airlines, reacted swiftly and effectively to the need for increased vigilance and security following the tragic effects of September 11th However, the burden of increased security measures has been considerable, with European airlines and airports paying out €3 billion for additional anti-terrorist security measures imposed by EU governments. This can be contrasted with the US, where industry has received an estimated US$32 billion in financial aid.

— Lack of review of security requirements: Layer upon layer of security measures are imposed on airlines but no review seems to take place to go back and verify the validity of previous measures when new ones are introduced. A good example of this was the continuing ban on metal cutlery despite the subsequent requirement to keep cockpit doors locked throughout a flight. Amendments to the rules on cutlery were only introduced after sustained lobbying from the airline industry. Virgin Atlantic believes that the Government should undertake a regular review of the validity of security regulations and measures.

— Scrambling of military aircraft in the event of a threat against civil aircraft: Virgin Atlantic is very concerned about the use of military aircraft to intercept civilian aircraft when a "bomb threat" is made against a particular flight. In these cases, where there is no threat of terrorists being on-board an aircraft, the scrambling of military aircraft actually worsens the safety environment. Virgin Atlantic strongly believes that the UK military's response to such events should be an appropriate and proportionate response to the perceived threat—we do not believe that this is the case at present.

One recent example of the lack of harmonised working within the UK Government is in relation to the notification of changes to UK threat levels. The Department for Transport has responsibility for advising airlines of changes to the "aviation" threat level, but at present there is nothing officially in place (with the Security Service or JTAC) for changes in the UK country threat level to be notified to airlines as they occur. This is a major cause for concern as often the data is "leaked" to the press, and airlines then have to try and verify it with the relevant government departments. The UK "country" threat classification is of importance to Virgin Atlantic as we have crew hotels in the UK, transport staff between UK airports, and are also responsible for managing threats against non-airport sited Virgin Atlantic assets. Aviation Security is much wider than just the airport/airside assets. In many respects the target-hardening of airside assets may force terrorists to attack soft targets such as check-in queues, airport forecourts and other areas where the public gather. As an airline is responsible for assessing threats made against us (including those targeting our non-airport based assets), it is vital that we have timely notifications of changes to both the "country" and "aviation" threat levels. In our view, the current system in place is unacceptable.

In the event of your committee deciding to conduct a wider inquiry into this issue, Virgin Atlantic would be more than willing to submit more detailed evidence. In the meantime, please do not hesitate to contact me if you require any further information on any of the points I raise above.

28 October 2005