EXPLANATORY MEMORANDUM TO

THE TRANSPORT SECURITY (ELECTRONIC COMMUNICATIONS) ORDER 2006

2006 No. 2190

1. This explanatory memorandum has been prepared by the Department for Transport (the Department) and is laid before Parliament by Command of Her Majesty.

2. Description

2.1 This Order extends the service provisions contained in a number of security-related enactments, to allow service by way of electronic communications as well as by hand or post. The modifications to the enactments extend the service provisions laid down in the relevant enactments to create two new methods of service by means of electronic communications. The first (which, except in the case of the Railways Act 2003, applies generally to anyone serving documents under the relevant enactments) involves sending a document by way of electronic communications; the second allows the Secretary of State (or others acting on his behalf) to post a document on a website and to give notice to the person on whom service is to be effected that the document is available there.

3. Matters of special interest to the Joint Committee on Statutory Instruments

3.1 None.

4. Legislative Background

4.1 This Order is made under sections 8 and 9 of the Electronic Communications Act 2000, which enable Ministers to modify any enactment for the purpose of authorising or facilitating the use of electronic communications.

4.2 This Order modifies a number of enactments relating to transport security, namely the Aviation Security Act 1982; the Aviation and Maritime Security Act 1990; the Railways Act 1993; the Channel Tunnel (Security) Order 1994 and the Ship and Port Facility (Security) Regulations 2004 (the relevant enactments).

4.3 The amendments to the provisions of the Railways Act 1993 relate only to documents served by the Secretary of State under sections 118 to 120 of that Act.

4.4 Regulations 20(2) of the Ship and Port Facility (Security) Regulations 2004 already provided for a form of service by way of electronic communications along the lines of the first method laid out in paragraph 2.1 above. However, given that it was necessary to amend those Regulations to introduce the second method of service described above, and that the Minister is empowered to make provision imposing conditions subject to which the use of electronic communications is authorised, a decision was taken to provide similar safeguards for electronic service as would exist in relation to other transport security enactments.

5. Extent

5.1 The Order applies to all of the UK. As set out in Article 11, an amendment effected by the Order has the same extent as the enactment amended.

6. European Convention on Human Rights

6.1 The Minister Stephen Ladyman, has made the following statement regarding Human Rights:

In my view the provisions of The Transport Security (Electronic Communications) Order 2006 are compatible with the Convention rights.

7. Policy background

7.1 The current practice of the Department's Security Directorate, (TRANSEC) is to send sensitive security information to industry by Royal Mail and a secure fax system called "Surefax". Both methods can be unreliable, slow and costly in financial terms. In addition, they are time consuming and labour intensive and have a negative impact on the environment. The two new methods of service (described in paragraph 2.1 above) introduced by the Order are consistent both with Government policy on providing government services electronically and with the Department's desire to provide more effective security communications.

7.2 The Department proposes to implement a "Secure Communications Project" whereby it will set up a secure website where it will post legal documents, advice, instructions and information. Recipients will be sent an email alerting them to the documents and informing them to go to the site. Some (though not all) of these documents are subject to prescribed methods of service laid down in the relevant enactments. Without the statutory amendments made by the Order, it would not be possible for such documents to be served by means of an email alert and posting on the secure website.

7.3 The Departmental Business Plan supports the drive to have the Secure Communications Project in place. It is also an objective of TRANSEC's Business Plan to aim for 95% of Directions/Instructions being served electronically by December 2006.

7.4 As well as internal consultation, the Department has consulted those departments with an interest in the relevant enactments or in secure communications (the Security Service, Cabinet Office, Department of Health, Department of Trade & Industry, the Health & Safety Executive and Department of Works and Pensions), from which no adverse comments were received.

7.5 Externally, the Department consulted its entire database of some 4,000 industry contacts involved in security matters, covering aviation, maritime and land transport, as well as our contacts in overseas Posts. In the consultation document, organisations were asked if, in future, they wished to receive all documentation from TRANSEC electronically. The Department received about 500 responses, of which only approximately 2 per cent of respondents did not want to move to the new system. Since the system is voluntary, they will continue to receive material using the current arrangements. Further details on the consultation process are set out in the Regulatory Impact Assessment.

8. Impact

8.1 A Regulatory Impact Assessment is attached to this memorandum.

8.2 There is no impact on the public sector.

9. Contact

Iain Ure at the Department for Transport, Tel: 0207 944 5146, e-mail: iain.ure@dft.gsi.gov.uk can answer any queries regarding the instrument.

Regulatory Impact Assessment

1. The Transport Security (Electronic Communications) Order 2006

2. Purpose and intended effect

Objective

- The objective of the Secure Communications Project is to disseminate information in a timely manner to relevant stakeholders. To enable this to happen, it is necessary to amend a number of Acts of Parliament, to streamline and vastly improve the current security communications links with industry. By doing so, it will allow the Department for Transport (DfT) to serve legal documents and disseminate policy advice, (some of which is classified – Restricted) using an electronic based system.

- The Order is made under sections 8 and 9 of the Electronic Communications Act 2000, which enable Ministers to modify any enactment or subordinate legislation for the purpose of authorising or facilitating the use of electronic communications. The Order will amend:
    a. The Aviation Security Act 1982
    b. The Aviation and Maritime Security Act 1990
    c. The Channel Tunnel Security Order 1994
    d. The Railways Act 1993
    e. The Ship and Ports Facilities (Security) Regulations 2004

Background

- The current practice of the Department for Transport's, Transport Security Directorate, (TRANSEC) is to send sensitive security information to industry by Royal Mail and a secure fax system called, Surefax. Both methods can be unreliable, slow and costly in financial terms as well as time consuming, labour intensive and have a negative impact on the environment.

- We propose setting up a secure website where we would post legal documents (e.g. 'Directions' to the aviation industry), advice (e.g. increases/decreases in threat levels), instructions (e.g. changes to the National Aviation Security Plan (NASP)) and information. Recipients would be sent an email alerting them to the documents and informing them to go to the site.

- The effect of moving to an electronic system would be:
    - To reduce the time taken in preparing and dispatching documents;
    - To save on resources;
    - To ease and speed up access to users, 24/7;
    - An assumption that all information would arrive safely, intact and to the correct end user;
    - To remove the need for users to follow up missing pages/documents;
    - To provide enhanced information facilities for stakeholders; and
    - To enable users to exchange information with the DfT electronically.

Rationale for government intervention

- The current methods for transmitting classified security related documents to the transport industry are outdated and no longer fit for purpose. They can be unreliable, slow and costly in financial terms as well as time consuming, labour intensive and have a negative impact on the environment.

- DfT is committed to meeting the Government's targets of delivering 100% of government services online.

- The Departmental Business Plan supports the drive to have the Secure Communications Project in place. It is also an objective set out in TRANSEC's Business Plan to aim for 95% of Directions/Instructions being served electronically by the revised date of 31st March 2007.

- There are strong indications that industry would welcome the proposed change and it would demonstrate that DfT/ TRANSEC are keeping up to date with modern forms of communication.

- Failure to proceed would give industry the impression that DfT/TRANSEC was not prepared to move with the times or meet its demands for faster, more accurate communications.

- The Secure Communications Project is a key component in the drive to improve efficiency through the use of technology and importantly, would be delivered in line with DfT's technical infrastructure.

3. Consultation

- Internally, we have consulted with the secretariats in TRANSEC involved in disseminating the information, plus IT Services Division (ITSD), Communications Division (CD) and the Departmental Security Officer (DSO). We consulted those departments with an interest in the Acts to be amended or in secure communications (the Security Service, Cabinet Office, Department of Health, Department of Trade & Industry, the Health & Safety Executive and Department of Works and Pensions), from where no adverse comments were received.

- Externally, we first consulted with about 40 organisations from our data base. We received 29 responses, none of which objected to the proposals. As a result of this endorsement, we then contacted our entire database of some 4,000 industry contacts involved in security matters, covering aviation, maritime and land transport as well as our contacts in oversees Posts. In the consultation, organisations were asked whether they wished to receive all documentation from TRANSEC electronically. They were informed that, in future, material would be placed on a secure website which could only be accessed by way of a user ID and Password and that they would be alerted to the need to access the material by way of an email.

- We received about 500 responses. Many firms welcomed the proposals and questioned why such a move had not taken place earlier. Around 2 per cent of respondents did not want to move to the new system and they will continue to receive material using the current system.

- In addition to the consultation, 'Newsletters' have been sent to internal and external stakeholders in order to keep them abreast of developments. The newsletters

prompted a few more companies to respond to the consultation.

4. Options

- The Order is necessary to support the delivery of a secure communications system, particularly the proper service of 'Directions'. As the five enactments currently stand, the service of documents has to be in a prescribed form, basically by hand, post or facsimile. There is currently no facility for service by means of electronic communications.

- In developing the policy for the new system four options were considered and extensively discussed with IT experts and the Secure Communications Project Board.

4.1 Do nothing

- Under this option we would continue with our current practice of sending sensitive security information to industry by Royal Mail and a secure fax system called, Surefax.

4.2 A stand-alone email server

- TRANSEC would send encrypted material, attached to email to a stand-alone email server in the stakeholder's office.

4.3 Virtual Private Network (VPN).

- A VPN is software hosted on two or more machines (e.g. PCs and/or servers), which forwards network traffic between them. The data exchanged between the machines is protected using encryption.

4.4 Stand alone Webserver (Preferred option).

- The system consists of a secure website on which could be posted material (Directions, threat advice, reports, etc). The receiver is alerted to the material by way of an email and accesses the site by user ID and Password.

5 Benefits

5.1 Do nothing

Benefits:
- Current system well used and tried;
- System familiar to all current users;
- No new equipment necessary;

Weakness:
- Current system is slow, unreliable and costly;
- Not what is wanted by the transport industry;
- The paper based system can be resource intensive and environmentally unfriendly.

Cost:

- There are no additional costs involved

This is not an acceptable option as it would leave the department with a poorly performing, time and resource consuming system of communication that is not a realistic option for moving forward. The demand for more efficient, secure communication is constantly increasing and will continue to be so.

5.2 A stand-alone email server

Benefits:
- Restricted material could be sent;
- Department would have total control of the system;
- We'd know if there were any transmission problems (server down);
- We could monitor receipt of the messages;
- We would have no 'firewall' restrictions;
- No additional equipment would be necessary, other than a normal computer;
- The cost of sending fax/post would be eliminated as would the cost of sub-contracted mailshots
- There would be environmental benefits (elimination of paper usage)

Weakness:
- Material may not get through the receiver's firewall;
- Up-front costs to receivers could inhibit take-up of the new system

Costs:
- Such a system would require receivers to purchase equipment, estimated to be in the region of £5k, plus maintenance/IT support charges.
- Administration of the system would be costly for DfT, though we are unable to quantify these.

5.3 Virtual Private Network (VPN).

Benefits:
- Accredited products readily available (hence least costly option for DfT)
- Little maintenance

Weaknesses:
- Physical network inflexible;
- Connections are dependent on receivers' IT systems being correctly configured;

Costs:
- In addition to some (albeit limited) costs to the DfT in customising the necessary software, such a system would require the purchase and maintenance of equipment at each receiver's location, and we are unable to quantify the costs involved

5.4 Stand alone Webserver (Preferred option).

Benefits:
- Greatly improved communications with the transport industry, including:

- Speed of direct communications between the DfT and industry would enable it to deal with events like 7/7 quicker;
- Current problems with sending material by fax/post would be eliminated;
- Stakeholders would only require access to a computer;
- Off-line and out of hours access;
- Ease of dissemination of information;
- Cost, administrative and environmental savings;
- The opportunity to extend alerts to a wider audience (e.g. Shipping);
- The ability to quickly/simply reach a large number of operators;
- The facility to develop an electronic library of information and advice;
- Possibility of including a facility that would allow industry to electronically send the DfT incident reports and the like;
- Incorporation of existing websites and others being developed, into the new site;
- The system would also aim to host other online databases, thus making the new standalone system even more effective and providing a saving;

Cost to the Department:

It is estimated that the project might cost DfT about £100-150k. (This is based on a study undertaken by an independent IT consultant) However, the exact amount will only become apparent once the specification is clearer and the System Development Team is in place. Also, there is a *strong possibility* that we would be able to adapt a system currently being developed within DfT to meet our requirements. *This would enable us to meet our requirements at a greatly reduced cost*. Discussions are on-going.

Set-up costs	£60-75,000
Network Support	£15,000p/a
Four Servers	£20,000
Consultant	£8,000
Hosting	The intention is for the Department to host the system.
Thereafter	£21,000 P/A ongoing support and network costs.

- Staff costs are limited to a proportion of the time of one G6 (Project Manager) together with ad hoc input from support staff (1 X G7, 1 X SEO, 2 X HEO). These costs are absorbed into the current headcount, but potentially there would be a need for a full time administrator to manage the system and work on the internet site (1 EO), when it is in place, which cannot be assessed until the trial is rolled out.

- There would be a proportional saving of admin staff time from the improved efficiencies in communicating and distributing of information to industry. This can not be measured currently but we would expect that we could realise some or part of a headcount saving from benefits of this evolving project.

- Time savings would arise from better communications.

Cost to industry (estimated);

- For individuals operating on their own or for organisations, a desktop or laptop, configured to meet the DfT's Code of Connection and standards, and under the control of a single, authorised and briefed user, is the recommended approach. A suitable firewall, which retails for under £300 for those who do not already have one installed, would also be required. It was only after study undertaken by an independent IT consultant that this cost became apparent, and so it was not known at the time of the consultation.

6. Small Firms Impact Test

- Our consultation exercise embraced organisations of all sizes and support for our proposals new system was overwhelming. The impact of the proposed changes on all businesses would be entirely beneficial as they would lead to the type of benefits detailed above. The new system would not be complex and is being designed to greatly simplify the system of communicating with industry as well as offering a facility for two way interaction with DfT. If an organisation decides not to opt in to the new system they would continue to receive communications by the current method.

7. Competition assessment

- The competitive market would not be affected by the proposed changes.

8. Enforcement, sanctions and monitoring

- Firms have the option of continuing to receive communications in the current form and not to be included in the new system. There would be no enforcement or sanctions as a result of the Order. However, built into the IT programme will be a system for monitoring if the recipient has opened the email alert. If after (a yet to be agreed) number of attempts the recipient has not opened the email the system will default to the next named contact.

9. Implementation and delivery plan

- It is planned to integrate a number of databases to create a master database for the project. Material would then be posted to the secure website. An email would be sent to a recipient, alerting them to material on the secure website. Access would be by password and user ID. We would monitor the delivery and action of the recipient. We plan to test the system by Christmas and go live, by the end of the financial year 2006/07. During the testing phase, we will issue instructions and guidance to users on how the new system will operate and will take account of any proposals/suggestions made by our stakeholders.

10. Post-implementation review

- As a matter of good practice, we will monitor the implementation of the new system and ensure that is delivering what internal and external stakeholders

expect. In time, we would hope for 100% take-up when the benefits of the new system can be demonstrated to users.

11. Summary and Recommendation

- Enabling of the Secretary of State and DfT to communicate directly with industry would greatly increase the speed and security of our communications process at little or no financial cost to industry. Option 4 below is therefore recommended.

Option	Total benefit per annum: economic, environmental, social	Total cost per annum: - economic, environmental, social - policy and administrative
1 Do nothing	- Apart no change from current working practices for TRANSEC staff, there in so benefit. - This is not considered to be an option.	No financial cost other than administrative. However, to maintain the current system would send a message to industry that DfT is unwilling to change and is content to maintain a system that is unreliable, slow, not secure and no longer fit for purpose.
2 A stand-alone email server	- Speed of transmission/receipt of information; - Information could be remotely accessed off site; -Restricted material could be sent; - TRANSEC would have total control of the system; - Transmission could be monitored and problems identified; - We receipt of the messages; - The cost of sending fax/post would be eliminated; -There would be environmental benefits from the elimination of paper.	- Those receiving material would need a dedicated computer. - The cost to the receiver would be in the region of £5k plus maintenance/IT support charges, which would be likely to inhibit take-up; - Material may not get through the receiver's firewall; - Administration of the system would be costly for DfT.
3 Virtual Private Network (VPN - software hosted on two or more PCs and/or servers that forward network traffic between them. The data is protected	- Least cost option for DfT; - Little maintenance; - Information can be remotely accessed.	- Receivers would be required to purchase dedicated equipment, which would be likely to inhibit take-up; - Transmission/receipt of information is slow; - The physical network is inflexible; - Connections are dependent on receivers' IT systems being correctly

using encryption)		configured with DfT; The DfT would need to fund the design and development of the necessary software, which would be costly.
4 Stand alone Webserver (By far the preferred option)	- Speed of communications; - Elimination of current problems with sending material by fax/post; - Off-line and out of hours access; - Ease of information dissemination; - Administrative cost savings; - Elimination in use of paper; - The opportunity to extend alerts to a wider audience (e.g. Shipping); - Ability to quickly/simply reach a large number of operators; - The facility to develop an electronic library of information and advice; - Possibility of including two way facility thereby allowing industry to electronically send report to DfT; - Incorporation of existing websites and others being developed; - The system would aim to host other online databases, thus making further a saving.	- Stakeholders would only require access to a computer and possibly an additional firewall (if not already installed) at a cost of less than £300. - We estimate that the Secure Communications Project could cost DfT somewhere in the region of £150k

12. **Declaration and publication**

I have read the regulatory impact assessment and I am satisfied that the benefits outlined in Option 4 justify the costs

Signed S.J. Ladyman.

Date 8th August 2006

Stephen Ladyman, MP

Minister of State
Department for Transport

Contact point for enquiries and comments: Iain Ure, Department for Transport, 5/15 Southside, 105 Victoria Street, London, SW1E 6DT, 020 7944 5146 iain.ure@dft.gsi.gov.uk