1. Purpose

1.1 This paper has been prepared jointly by RSSB and Network Rail and is intended to inform discussion concerning a proposed new activity for RSSB in relation to cyber security of the railway.

2. Background

2.1 Cyber security is the security of cyberspace. The Cabinet Office UK Cyber Security Strategy defines cyberspace as ‘…an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the other information systems that support our businesses, infrastructure and services.’

2.2 The Department for Transport (DfT) has asked RSSB to ‘establish an information portal on existing RSSB websites to raise awareness of cyber issues across the rail industry and publish useful information and related links’.

2.3 Further to this, RSSB is requested to work with the industry to assess the need for rail-specific standards and guidance on cyber security to inform the agreement with industry of a standards development programme.

2.4 This is a new ‘function’ for RSSB under the Constitution which has resource and funding implications for the company.

2.5 The draft request from the DfT is attached as Annex A to this paper.

3. Risks to the railway

3.1 The Government’s 2010 National Security Strategy rated cyber-attacks a ‘Tier One’ threat alongside, Terrorism, War and Pandemic disease. Reports of cyber-attacks in the media are growing and the UK Intelligence Agencies are reporting a high degree of risk to UK and European transport infrastructure including rail.

3.2 Cyber security is relevant to the railway in various technology domains, including rail control systems, asset management systems, business systems, telecommunication networks and embedded software, both in fixed infrastructure and on trains.

---

1 The UK Cyber Security Strategy, Protecting and promoting the UK in a digital world, Cabinet Office, November 2011
3.3 The current risk to the railway is still emerging as advances in technology are exploited by all parts of the sector to improve performance, safety and value. This includes a shift from legacy systems using proprietary systems to greater use of standardised technologies, protocols and operating systems. Interconnectivity between systems greatly improves their value, but also increases their susceptibility to cyber-attack.

3.4 Loss of security of a system does not equate to an unsafe condition, however there is a close relationship between security and safety. Compromised security could lead to unsafe events, both directly and indirectly.

3.5 The traditional approach of operational railway systems failing safe mitigates some risk, but the consequential impact of this and continued degraded operation of the railway introduces new risks. Increasingly, as these systems become more complex, reliably achieving failsafe conditions is more difficult, especially when subject to a cyber-attack.

3.6 Risks are not limited to safety. Cyber security has the potential to affect the whole supply chain and rail businesses need to take into account not just their own arrangements, but also consider the resilience of key suppliers. Failures in the supply chain, especially those that may persist for a few days, can quickly have a direct operational impact.

3.7 There is reputational and commercial risk, especially where attacks affect passengers and freight customers, for example as a result of operational failures, or failure of ticketing and revenue systems.

3.8 Media interest in cyber security has the potential to give wide exposure to relatively minor incidents. The industry’s response to a cyber-attack against the railway will be played out in public and will have a high impact on passenger trust in the system.

4. Mitigation

4.1 To aid mitigation of this risk, DfT has asked RSSB to raise awareness of cyber issues across the rail industry by promoting information and links on RSSB websites and work with the industry to assess the need for rail-specific standards and guidance to inform industry agreement on a standards development programme.

4.2 The standards development programme is not necessarily limited to RSSB-produced material and could include contributions from other organisations, including Network Rail, with RSSB providing a coordination and facilitation role.

4.3 A growing number of non-specific standards for cyber security already exist or are in development, which will need to be taken in the context of the railway.

4.4 There are parallels with the management of safety; security needs to be designed in as part of systems and processes and be part of the culture that drives risk aware behaviours.

4.5 RSSB has significant experience in supporting and improving the industry’s management of safety including providing standards, tools and other material; this approach could be used for cyber security matters, but this will be starting from a lower level of industry understanding.
4.6 The High Integrity Software Group, under the System Safety Risk Group, has shown a strong interest in cyber security and RSSB has supported cyber security initiatives as part of work supporting the ERTMS Programme.

4.7 This work will support the Industry’s strategic objectives for security and will also contribute to safety, performance and wider business sustainability in the knowledge that existing systems are unlikely to be sufficiently resilient in the future.

5. Implications for RSSB

5.1 Resourcing
5.1.1 RSSB will need to develop expertise and is likely to need to increase resource to undertake this additional work.

5.2 HSE impact
5.2.1 There are no specific health, safety or environmental issues for RSSB as a result of this work.

5.3 Legal
5.3.1 It is likely that output from this work will, by design, be made widely available. However, in developing and managing the work it is possible that there will be a need to restrict some information. Systems and processes will need to be adapted to accommodate this and there is a possible requirement for some personnel to have appropriate security clearance.

5.3.2 Liabilities are anticipated to be similar to other aspects of standards production, subject to a possible increase in resource dependent on the extent to which RSSB undertakes this work.

5.3.3 The intellectual property is likely to be documented in publically available material, but the development of this material and associated intellectual property is possibly a marketable capability in its own right.

5.4 Finance
5.4.1 As this is potentially a new area of activity the expenditure and possible income are unknown at this stage. If supported, for the 2014/5 financial year the cost is expected to be approximately £100k, but this could rise in subsequent years depending on the scope of work and the extent to which other industry partners produce relevant material.

6. Recommendations
6.1 The board is asked to:

- DISCUSS the issues around cyber security and whether RSSB should equip itself to meet DfT request
- DECIDE whether to take it on, and if so pass a
- RESERVED RESOLUTION to adopt the function of developing a programme for cross-industry standards for cyber security
Annex A: Draft letter from DfT

DRAFT FOR COMMENT

Department for Transport

Chris Fenton
Chief Executive Officer
RSSB
1 Torrens Street
London
EC1V 1NY

Dear Chris,

Development of Industry Cyber Security Initiatives

The Government’s 2010 National Security Strategy rated cyber-attacks as a ‘Tier 1’ threat and significant resources have been allocated to develop our response across all national infrastructure facilities.

Within the Department, it has been identified that the Rail industry will face increasing exposure to cyber threats as we become ever more dependent on interconnected and remotely accessible control and communication systems. The more frequent deployment of commercial off-the-shelf technologies, with interfaces to legacy systems having few or outmoded security features will exacerbate the problem. It has also been identified that knowledge of the relevant issues within the industry is generally immature, and that the level of risk and appropriate mitigations are not well understood.

The Department has commissioned further research that will inform the development of policy and supporting guidance to industry that is expected to be available later this year. Given RSSB’s unique operational partnership with the industry we believe that it is ideally placed to help educate the industry through the promulgation of information and good practice, and further support the industry in the development of formal standards and codes of practice as appropriate.

My team has had initial discussions with established contacts in RSSB who have indicated that they would be able to support these initiatives. Initially the work would involve the establishment of an information portal on existing RSSB websites to raise awareness of cyber issues across the rail industry and publish useful information and related links.

Following on from this, and in parallel with the development of Departmental policy, we would envisage RSSB working with the industry to assess the need for rail-specific standards and guidance, covering both resilience measures and the processes and methods needed to manage cyber security. The conclusion of the assessment would inform the agreement with industry of a standards development program.
DRAFT FOR COMMENT

I would ask that you confirm RSSB’s support for this important initiative in order that my team can proceed to develop the necessary work streams with the appropriate RSSB personnel.

Please contact me if you have any further queries on this matter.

Yours sincerely,

Robin Groth