AGENDA ITEM:  C1

MEETING:  RSSB Board Meeting
DATE:  06 November 2014
SUBJECT:  Cyber Security update
SPONSOR:  Anson Jack
AUTHOR:  Andy Goodwin

1. **Purpose of the paper**
   At the May board a reserved resolution was passed to adopt the function of supporting the industry on cyber security. The purpose of this paper is to update the board on the progress made to date.

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) 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 was 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.

3. **Summary of progress**
   3.1 The role of developing the actions was picked up by the existing High Integrity Software Group (HISG) which consists of a broad cross-industry mix of technical specialists. This group has worked collaboratively to complete the first action to establish an information portal on the RSSB website. A list of key members of the group are listed as Annex A which shows good representation from across the industry. The material for the website has been approved by the HISG and the portal is on course for a launch date in November.

   3.2 To date it has involved around 10 man days of RSSB technical input plus at least the same again from experts across the industry/Government.

---

1 The UK Cyber Security Strategy, Protecting and promoting the UK in a digital world, Cabinet Office, November 2011
3.3 A detailed communications plan is in place:

- Pre-launch presentation to SSRG supported by Peter Gibbons (Head of Cyber Security at NR)
- Post Launch presentation to ISCC and cascade to Standards Committees
- Post Launch presentation to TLSG and cascade to SICs
- Post Launch presentation to CENELEC TC9X
  (European standards committee responsible for railway technical systems)

4. **Next Steps**

4.1 The HISG is considering further steps which will be reported to the board in 2015.

4.2 Initial feedback is that there is sufficient published material in existence on Cyber Security and what is missing is advice as to what to apply and when. The HISG is considering future needs including potentially whether there is further scope for sharing of best practice and whether ‘security integrity levels’ should be developed for rail industry application.

5. **Recommendations**

5.1 The board is invited to:

- **NOTE** the progress to date and that a further update will be brought back to board in 2015.
Annex A: Key members of the High Integrity Software Group

Network Rail – Peter Gibbons (Head of Cyber Security)
ROSCOs (Porterbrook) – Simon Tonks
Suppliers – Francis How (RIA) and Andy Pankhurst (Alstom)
Centre for Protection of National Infrastructure (CPNI) representative
Adelard – Robert Stroud
Department for Transport – Dermot Carroll and Rob Evans
Train Operators – Nick Hortin (First) and Simon Green (Southern)
ORR – Paul Frary and Brian Ellis