Post Office / Fujitsu Review Meeting

Security Liaison

Thursday 26 June 2008

11:30 to 13:30, Fujitsu, Bracknell

(Meeting ref: 0608)

Meeting Called By:	*Sue Lowther*			
Present:				
Attendees:			**Deputies:**	**Apologies:**
Sue Lowther [SL] Paul Halliden [PH]	Howard Prichard [HP] Brian Pinder [BP] Pete Sewell [PS] Fiona Woolfenden [FW]* David Cooke [DC]* * Item 6 only.		N/A	Alan Simpson [AS]

Minutes

	Agenda Item	Discussion, Actions Arising & Decisions Taken
1	**Review of Previous Minutes**	No comments on previous minutes. Progress on actions covered under relevant agenda item below.
2	**Security Policy**	1. HP reported the RMGA policy had been updated following Post Office comments. It has been sent out for internal Fujitsu review (Post Office Information Security has an informal copy). The date for Fujitsu comments is now passed. Hillary Forest (Fujitsu Commercial) had raised some minor comments that needed resolving. An updated version with comments resolved will be formally issued to Post Office by 4 July. **Action BP.** **BP: All comments outstanding form have been addressed and the policy is now out and awaiting approval with Acc Dir.** D:\ SVMSECPOL0003.doc 2. HP would like to get a version of the policy formally approved as the HNG-X project was currently progressing in a policy vacuum. PH reminded him that the policy is critical for acceptance and an incomplete policy might fail even if approved. HP replied he believed all significant issues raised by Post Office to have been

		3. addressed. 4. Post Office are also updating the Community Information Security Policy (CISP). A first release has restructured it to follow the updated ISO17799 and hence ISO 27001. This version has been formally released for comment. No comments were received. It will now be updated to reflect the changes for HNG-X. A round table review will be organised with Fujitsu when the document is complete. **Action PH**
3	**ISMS Manual**	1. There was some discussion about ensuring the (non-contractual) ISMS Manual and the (contractual) service description aligned with each other and with the service to be provided. It was agreed to do this in a two step process: a. Align the ISMS Manual with the existing Service Description for HNG-X. **Action BP.** **A review of the ISMS is underway a meeting is arranged on Mon 4th Aug to address the first step of ensuring the ISMS accurately reflects it's objectives and compliments the security service description SVM/SEC/SD/0017. (BP)** b. Review the Service Description and align both it and the ISMS Manual with the service to be delivered raising a Change Request to cover and changes. **Action: HP to initiate.** **The Service description SVM/SEC/SD/0017 is a CCD and describes the service the security team currently provides. A review /update of this document is underway to ensure it accurately reflects the service the security team currently provides. (PS)** ***NB: The ISMS Manual does not replace or enhance the Security Service Description document in any way. It is a separate and local document which describes a high level overview of the approach and framework (known as ISMS) used within RMGA Security.***
4	**Security Improvement Plan**	1. The report(s) identifying progress against the SIP and the HNG-X Risk Treatment Plan had not been circulated before the meeting. ***NL Sent the IG Pack out prior to 10th June this included the SIP.*** ***BP Sent Mar/Apr/May RT Matrix to DK prior to 23 Jun 08.*** 2. Circulation of the monthly reporting pack for this meeting still seems problematic. It was agreed that it could be sent to SL in plain and to

		3. PH as a self-extracting password protected file. The password would be texted separately. **Action BP**. **Disagree: Did we all agree to this?** **I thought I only agreed to send the SOA as a PGP to PH.** **I did this on 27/06/08 'as promised'.** **I think this entry by PH may be incorrect. Your views?** 4. Post Office have still not seen or agreed the terms of reference for this series of meetings (an action on Fujitsu in the Security Improvement Plan). HP assured the meeting they had been prepared. He will distribute a copy for comment. **Action HP**. **2 Docs currently in DIMENSIONS** **ISMF ToR's Out for Internal Review** **ISMR ToR's Out for Internal Approval.** D:\profiles\Pinderb\Desktop\RMG ISMF T D:\SVMSECSTD0027.doc 5. The updated plan showing progress towards ISO 27001 certification had also not been circulated as promised last meeting. **Action HP** ???? 6. BP reported the scope had now been finalised and would remain static until reviewed in 12 months. SL reminded him of the need to review the scope on major changes prior to that date and asked for a copy of the scope. Both points were agreed. **Action BP**. **Copy sent to DK as promised (PGP'd) 27/06/08** 7. SL asked HP to comment on a rumour that RMGA did not intend to seek formal certification against ISO 27001. HP assured her the rumour was untrue; the audit by BSI is still planned for August. **In view of staff sickness/leave etc this may be delayed to September???**
5	**Security Incident Response Plan**	1. PS reported he has produced a plan covering PCI-related incidents for RMGA in conjunction with Richard Barber. Richard had also produced one for Post Office Limited. A combined HNG-X business continuity plan is now being developed. There will be a walk-though to ensure consistency.

		2. Connie Penn had raised a concern that the plan was a disaster recovery plan and that business continuity is not fully addressed, especially with reference to testing of the plan. HP reported he had discussed the issue with Connie and there is now agreement. 3. SL apologised for not joining the previous day's rehearsal. The dial-in details provided did not work. 4. Meetings are being set up to rehearse the Elective Disconnect process (switching off one data centre).
6	**HNG-X Acceptance**	1. FW had prepared a series of document summarising the position on Document Review acceptance "tests" for security. 2. Sensitive documents (such as the Statement of Applicability) which have a restricted circulation will be sent password protected direct to PH rather than via the RMGA and HNG-X document management systems. **(Actioned as stated above BP)** 3. SEC-3255 requires criminal record checks by RMGA. BP reported they will be required in a revised HR policy awaiting internal approval. The new document will be submitted to Post Office and be cross-referenced in the RMGA Information Security Policy. **Action BP.** **A meeting has taken place with HR and GS. Process documentation by HR, plus licensing for software is underway. A review of this will take place around 20th Aug and completion date expected to be 1st September.** 4. SEC-3082 seems to have got the wrong defect note attached to it. PH clarified what the defect was. He will agree a way of correcting the error with Neil Williams (Post Office). **Action PH.** 5. More details in the post-meeting notes circulated by FW.
7	**AOB**	1. None raised.
8	**Agree date and location of next meeting(s).**	31st July, and 2nd September in Bracknell. There will be a section at the end of each meeting to review acceptance progress.