ANNUAL SECURITY REVIEW - DATA COMM NETWORKS

Instructions:

1. PURPOSE OF A REVIEW: Section 4.901 of OP113, Protection of Electronic Information (see also SW910 Section 3.43), requires an annual security review of each electronic system's environment, hardware, software, operating procedures, and documentation. A proper review ***SHOULD*** provide direction on how to maintain and/or increase the level of a system's information protection.

2. PERFORMING A REVIEW: The annual review ***MUST*** be coordinated between the SWBT employees and/or agents who support the DCN (e.g., Security or System Administrator, Application Manager, Business Flow Process Specialist, etc.). These functions/jobs are further defined in OP113.

3. ITEMS TO BE REVIEWED: The following pages describe the areas from SW910 to be covered in each annual review (in subsequent releases, [number] indicates a question from the previous SW910). Any concerns or issues unique to a given DCN ***MUST*** be referred for resolution to the SWBT experts for the DCN. Complete the questions by filling-in the following:

    - TRACKING INFORMATION: Review date, name/location of the DCN, name/phone number of the primary reviewer or a local contact

    - COMPLIANCE STATUS: The status of each question - "Yes" (in compliance), "N/A" (not applicable), or "No" (a deviation).

    - ATTACHMENTS: BOTH "N/A" and "No" answers ***MUST*** have an attached explanation (e.g., item is NA because of substitution of approved physical protection in place of software protection, ISF representative has reviewed and agreed protection step is not needed, exception report is being forwarded, etc.).

4. DOCUMENTING DEVIATIONS: In accordance with SW910, Section 3.45, exceptions ***MUST*** be fully documented and resolved as soon as practicable. If a requirement is considered unnecessary, unreasonable, or not possible, review it with the organizational ISF representative. For significant deviations, a written exception and plan for correction ***MUST*** be approved by the organization's Director, retained for the life of the system (i.e., available for audit reviews), and a copy sent to the ISF Chairperson at the address listed in the SWBT electronic Blue Pages (PHONE option B) under Interdepartmental Security Forum, or by E-mail to "isf" on system "isoa."

5. QUESTIONS: Hardware and software questions ***SHOULD*** be referred to the appropriate SWBT specialists. Questions or comments on policies or procedures may be referred to the appropriate ISF representative or the ISF Chairperson as listed in item 4 above.

Security Admin/
Dept. Coord.: _____ Phone: _____

Review Date: _____ Data Comm Ntwk: _____

SW910 SECT	SECURITY AREA/REQUIREMENT - COMPLIANCE (Answer YES, NO, or N/A; Explain if N/A or NO)	
AREA: Security Responsibilities		
2.03	1. Is a Security Administrator assigned with duties documented?	
2.03	2. Has the Security Admin or organizational contact completed training for general security and the platform being used?	
2.03	3. Is the Security Administrator or organizational contact registered with the ISF representative?	
AREA: Integrity Controls - Hardware and Physical Environments		
3.02	4. Is there appropriate control of physical access to hardware/software?	
3.04	5. Is appropriate earthquake protection in place?	
3.05	6. Has the annual environmental review of processing location been completed and documented?	
AREA: Integrity Controls - Software and Data		
3.06	7. Is the software change control process documented & reviewed for compliance?	
3.06a	8. Is all DCN software authorized, ownership documented, appropriately licensed and acquired?	
3.06b, 3.06c	9. Is developing, copying, or using software or mechanisms to bypass security prohibited?	
3.07	10. Is the software backup process documented & reviewed for compliance?	
3.07	11. Is a copy of critical data maintained and OP47 retention guidelines reviewed for compliance?	
AREA: Access Controls - Session Management and Transport		
3.12	12. Are Transport security processes used whenever possible?	

Review Date: _____ Data Comm Ntwk: _____

SW910 SECT	SECURITY AREA/REQUIREMENT - COMPLIANCE (Answer YES, NO, or N/A; Explain if N/A or NO)	
3.13	13. Are inactive terminals/input devices timed-out or locked-up (e.g., after 15 minutes of inactivity)?	
3.13	14. If a session is interrupted (e.g., user hangs up without normal logoff, etc.), is re-connection prevented without another logon?	
3.14	15. If a trust level 1/0 system is directly accessed from a dial-up or untrusted facility, is a token card or biometrics required?	
3.14	16. Are unprotected dial-ups controlled on a session-by-session basis?	
3.15	17. Do employees understand and comply with the restrictions on giving dial-up or system access information to unknown persons (Social Engineering)?	
3.16	18. Is security information (e.g., passwords) encrypted before being transmitted over the DCN?	
AREA: Identification Controls - Userids		
3.17	19. Is each user assigned a unique userid?	
3.17	20. Are SWBT standard userid formats required?	
3.19	21. Is a documented process used to approve all new users?	
3.20	22. Is sharing of individual userids prohibited (no group userids)?	
3.21	23. Are this system's userids identified in SUITS with this system?	
3.21	24. All userids reviewed for validity at least monthly (using SUITS)?	
3.21	25. Non-SWBT userids re-authorized by SWBT sponsor every 90 days?	
3.21	26. Does SUITS or DCN cause re-authorization of all userids at least every six months (e.g., list of users sent to the users' SWBT manager)?	
3.22	27. Are default and vendor supplied userids strictly controlled (e.g., removed or invalidated)?	
AREA: Authentication Controls - Passwords, Tokens, Biometrics		
3.23	28. SWBT policy against sharing personal passwords implemented?	
3.23	29. Has the SWBT policy against supervisors having a list of employee private passwords been implemented?	
3.24	30. Entire authentication process required even if the userid is invalid?	
3.24	31. User required to fully authenticate himself before changing his password?	

Review Date: _____ Data Comm Ntwk: _____

SW910 SECT	SECURITY AREA/REQUIREMENT - COMPLIANCE (Answer YES, NO, or N/A; Explain if N/A or NO)	
3.25	32. Using OP113 password format (6-8 characters, not blank or a repeat of the userid, at least one letter and at least one number/special character not in first/last position)?	
3.26	33. New/administratively assigned passwords changed at first access?	
3.27	34. Is the plain text display of passwords suppressed during logon (i.e., on input devices or printers)?	
3.27	35. Are passwords on password files encrypted and access restricted?	
3.28	36. Are user passwords automatically expired (e.g., each 31 days)?	
3.29	37. Is a user prevented from reusing the same password (e.g., for 6 changes/months)?	
3.30	38. Are tokens/one-time password devices registered?	
3.30	39. Are tokens re-authorized by SWBT management each 6 months (e.g., in a similar manner to userids)?	
AREA: Authorization Controls - Controlling Access to Resources		
3.31	40. Is access to non-SWBT networks and systems limited to official SWBT business?	
3.33	41. Are privileged system/application userids carefully controlled?	
3.33	42. Is access to access control files limited to authorized users?	
3.33	43. Operating system file access restricted to authorized users?	
3.34	44. If requested, can userid authorization be given as part of a group?	
3.34	45. Do system's defaults restrict access to creator of new files/data?	
AREA: Monitoring and Control Functions		
3.36	46. Is the audit log protected from unauthorized access?	
3.36	47. Is every significant event (e.g., unauthorized access attempts) logged & the log retained (paper/mechanized copy) for at least 90 days?	
3.36, 3.37	48. Are system logs reviewed & unusual or suspicious events reported?	
3.38	49. Is a SWBT warning banner displayed at point of initial entry?	
3.39	50. Is the logon session terminated after 3 consecutive invalid attempts and the Sec Admin notified?	

Review Date: _____ Data Comm Ntwk: _____

SW910 SECT	SECURITY AREA/REQUIREMENT - COMPLIANCE (Answer YES, NO, or N/A; Explain if N/A or NO)	
3.40	51. Is the last valid logon date/time and number of unsuccessful logon attempts displayed after a successful logon?	
3.41	52. Is CSAG's weekly E-mail list of invalid userids used to inactivate these userids?	
3.41	53. Inactive userids reviewed for deletion (e.g., no usage for 90 days)?	
AREA: Reviewing System Security		
3.44	54. Has the Trust Level been determined for the data and services connected to this DCN (0 - Strategic/Mission critical data or services; 1 - Restricted-Proprietary data or services; 2 - Proprietary data or services; 3 - Internal but non-sensitive Company data; 4 - Data or services available to the public)?	
3.45	55. Are OP113 exceptions documented & reviewed annually?	
AREA: Contingency Planning		
4.07	56. Do user organizations have documented interim contingency procedures for how they would do business without this system?	