MEETING MINUTES & REPORT OF THE LOG FILE RETENTION TASK GROUP TO THE ERC

19 JANUARY, 2000

Attendees: Charles Arp, OHS; David Bussard, Ohio Public Works Commission; Scott Eitel, DAS; Laurie Gemmill, OHS; Jerry Howard; ODI; Myron Kaliski, ODRC; Jason Mather, Office of Criminal Justice Services; Dennis Mitchell, ODRC; Melissa Peters, ODRC; Greg Schneller, DAS; Tracy Smith, ODRC; and Daryl Weir, Legislative Information Systems (chair).

The group was called to order at 2:30 p.m.

The IT General Schedules for Computer Operations and Technical Support were distributed and the group reviewed IT-OP-06 to IT-OP-12 and IT-CS-01.

Discussion focused on the suitability for the technical community of these recommended retention practices.

- Points raised:
    - Need better definition of the term Entity "system backup cycles"
    - Should logs of inbound traffic be separated from outbound traffic in the schedules?
    - Should inbound log files be protected by Open Records Law for privacy purposes?
    - Security logs should be exempted from Open Records Law
    - Backup cycles vary depending on factors such as mission criticalness of data, machine type (e.g. PC vs. mainframe), backup medium
    - Which issues should be addressed through the IT General Schedules and which should be handled by the DAS Office of Policy and Planning either through draft legislation or policies?

- The group decided on submission of these recommendations to the Electronic Records Committee:
    - Change retention statement of IT-OP-06 System Backup Files to "Retain for a minimum of 12 system backup cycles, then destroy."
    - Change retention statement of IT-OP-12 Audit Trail Files to "Retain for a minimum of 12 database/master file backup cycles, then destroy."
    - Change IT-OP-08 Computer Usage Files to "Retain until no longer of administrative value to agency, then destroy."
    - Remove words "then destroy" from all IT General Schedules prompting agencies to address issue of retaining an archive of computer files.

Further, the group decided on these recommendations for the Electronic Records Committee to submit to the DAS Office of Policy and Planning:

- State operations could be compromised if security logs, passwords, certificate authorities, IP addresses, router information, security architecture and other primary data is available to the public under the Open Records Law. Strongly urge OPP to draft legislation excluding these types of data sources from being publicly available.

- Privacy of individual citizens can be violated if log files are publicly available. Strongly urge OPP to draft legislation excluding log files from being publicly available while providing public access to aggregate data.
- State agencies are in need of guidance and assistance in responding to suspected security breaches. Strongly urge OPP to work with DAS and Ohio Highway Patrol to create a team to respond to security violations.

Having completed its mission, the meeting was concluded at 4:30 p.m.

No further meetings of the task group are planned. Daryl Weir, Chair of the Log File Retention Task Group, will present these recommendations to the Electronic Records Committee at its next meeting on February 15, 2000.