A97 Evaluation of Audit Trails and Security Features in Software Systems

Valerie K. Bostwick, MS, Jacqueline M. Jarzombek, BS, Mallory Mest, BS, and Terry W. Fenger, PhD, Marshall University Forensic Science Center, 1401 Forensic Science Drive, Huntington, WV 25701; John Paul Jones, MBA, National Institute of Justice, Office of Science and Technology, 810 7th Street, North West, Washington, DC 20531; and Rhonda K. Roby, PhD, MPH, NES Project, 3500 Camp Bowie Boulevard, Room 310, Fort Worth, TX 76107*

After attending this presentation, attendees will acquire a broad knowledge of the different audit and security features offered in a variety of software programs. Participants can use this knowledge base in helping them choose a software system for their laboratory.

This presentation will impact the forensic community by increasing awareness of the audit trails and security features available in different software systems.

The use of software systems in forensic DNA testing has played an integral role for years in DNA analysis, even with RFLP sizing. And even more recently, LIMS and expert systems are being validated and adopted into the workflow of forensic DNA laboratories. With the increase in electronic automation, the advances in paperless systems, and the development of software tools, sophisticated algorithms and audit trails are being introduced. As DNA data analysis becomes more automated in processing, the evaluation of proper documentation and user tracking is essential. In court, it is crucial when an analyst makes a change to an allele call, that it be traced to the analyst who made it. When looking at software systems, security features such as analyst login, administrative control, and audit trails should also be evaluated to ensure they meet the laboratory's quality assurance requirements.

The NIJ Expert System Testbed (NEST) Project Team has evaluated several single source expert systems and mixture deconvolution tools including: DNA_Data Analysis Software (United States Army Criminal Investigative Laboratory, Fort Gillem, Georgia); FSS-i3™ Expert Systems Software version 4.1.3 (Promega Corporation, Madison, Wisconsin) in conjunction with GeneMapper® *ID* Software version 3.2 (Applied Biosystems, Foster City, California); GeneMapperâ *ID* Software version 3.2 (Applied Biosystems); GeneMapper® *ID-X* Software (Applied Biosystems); TrueAlleleâ Databank version 2.9 (Cybergenetics, Pittsburgh, Pennsylvania); and TrueAllele® Casework System Package (Cybergenetics). All of these software systems offer different tracking and administrative control features. When launching the software, some systems have unique user login and password requirements, while other software programs require entering a user ID at an alternate point during sample analysis. There are also software programs that track the Windows user login, and associates that user with a data set imported into the software. The number of software licenses purchased may dictate which type of user tracking best fits the laboratory.

Audit trails document the user logged in, changes made by the user, and the rules that fired, to name just a few examples. Each software package reports different information in its respective audit trails. Another level of security examined is the accessibility of settings to various users. There are software packages that allow the administrator to limit access to custom settings, and some that do not. For example, if the laboratory's quality assurance program states that only an administrator or a technical leader can modify settings and thresholds, access to these settings can be controlled in some software packages.

The intent of this presentation is to inform the forensic community of the differences in security and audit features in single source expert systems and mixture deconvolution tools. The information presented in this poster may assist a laboratory in choosing not only a software program that meets both its analytical needs but its security needs as well. Comparisons between the software packages will be discussed, highlighting the benefits as well as possible areas for improvement for each program assessed.

This project was supported the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in this presentation are those of the authors and do not necessarily reflect those of the Department of Justice.

Expert Systems, Audit, Security

 ** Presenting Author*