Who is SWGDE and what is the history?

Mark M. Pollitt
[Former] Chair, SWGDE
1/22/03

The Federal Crime Laboratory Directors group formed SWGDE in 1998. It was noted that the traditional audio and video examination and processing was becoming digital and, along with digital still photography, was converging with computer forensics. As a result, they formed a group to explore digital evidence as a forensic discipline. The initial members were the forensic laboratories of the ATF, DEA, FBI, IRS-CID, US Customs, US Postal Inspection Service, and the US Secret Service. In addition, NASA and the Department of Defense Computer Forensics Laboratory participated from the beginning. In an effort to widen the participation, representatives from North Carolina, Pennsylvania, and Illinois State Crime Laboratories were invited to participate along with the Florida Department of Law Enforcement. Later on, representatives of other state and local agencies (including Ocean City, Maryland and Lakewood, Colorado) were accepted for membership.

Many of those state and local agencies discovered and joined SWGDE by attending a presentation given at IACIS, HTCIA, GMU, as well as announcements sent to IACP and various e-mail lists. It should be noted that the members of SWGDE individually have many years of digital forensic experience. Most of the members of SWGDE are members of prominent organizations such as American Academy of Forensic Science, IACIS, HTCIA, and IOCE, and many are officers of these organizations.

Early discussions revealed that, in fact, there were many similarities and overlap in the disciplines of audio, video, image analysis and computer forensics and that it was desirable to develop standards and harmonize operations among these disciplines. As a result, the Scientific Working Group on Digital Evidence was formed, under the same umbrella that covers the Scientific Working Groups on DNA (SWGDAM), Questioned Documents (SWGDOC), Trace Evidence (SWGMAT), Drugs (SWGDRUG), Fire and Explosives (SWGFEX), Fingerprints (SWGFAST), and Imaging (SWGIT). For further information concerning scientific working groups see the Forensic Science Communications article by Dwight Adams1

SWGDE is focused on the practice of digital evidence forensics primarily in the laboratory setting. However, we have endeavored to adopt documents that will be useful to agencies that perform these tasks in a non-traditional forensic laboratory or the field. Some of SWGDE's earliest work explored the principles of digital forensics and developed some baseline definitions. In 1999, SWGDE adopted a set of principles and definitions that the group felt were as close to universal as possible. These principles were published in the Forensic Science Communications2 and submitted in October, 1999 to the International Organization on Computer Evidence (IOCE). The IOCE meeting was held in connection with a major conference: the International High Tech Crime and Computer Forensics Conference. Delegates at that meeting used SWGDE's

material, as well as material contained in the United Kingdom's Association of Chief Police Officers (ACPO) Best Practice Guide, to form the IOCE Principles. IOCE adopted the SWGDE Definitions verbatim. In turn, the G-8 High Tech Crime Sub-Group used the IOCE principles and definitions as the basis for the G-8 Digital Evidence Principles3. From 2000 onward, SWGDE has worked closely with the American Society of Crime Laboratory Directors (ASCLD) and the companion organization, ASCLD Laboratory Accreditation Board (ASCLD/LAB). Over this period of time, SWGDE cooperated with ASCLD/LAB and proposed adding Digital Evidence to the list of "accredited" disciplines. ASCLD/LAB accredits crime laboratories on a voluntary basis4. While the ASCLD/LAB guidelines are copyrighted, at the time of this writing, the proposed changes, including the addition of Digital Evidence as an accredited discipline, are available on the ASCLD/LAB website5.

The ASCLD/LAB Delegates, who are the Directors of all ASCLD/LAB accredited labs, have voted to accept the proposed revisions. When reading the document, it is also important to recognize that "Digital Evidence" does include digital video/imaging and digital audio examinations. The wording within the document is to be inclusive of these fields. One example of which is the inclusion of "spectra", which is very common in the audio analysis discipline. One should note that each item in the ASCLD/LAB Manual is marked with a notation of E, I, or D. These represent essential, important and desirable criteria. Compliance with items marked with an "I", such as the educational requirement for a Bachelor's degree, are only required in 75% of criteria6.

The Best Practices document that is up for discussion at this time is a companion document that is designed to provide guidance for laboratories who either have, or are contemplating having digital evidence units (computer, audio, video or digital imaging) accredited. It is not focused on non-traditional labs, investigative units or individual practitioners. We welcome suggestions from those groups, however.

Like the ASCLD/LAB Manual, the Best Practices document seeks to provide a framework for agencies to insert their own criteria. ASCLD/LAB describes what should be included in a protocol, but does not specify any particular format or content. Neither document sets standards per se, but rather lists the issues that need to be addressed. If one of the issues does not apply, then it can be documented that it does not apply to the particular situation. Accreditation is about process, not particulars. It is also important to note that the Best Practice document was written intentionally vague in some areas. This is to allow individual agencies the ability to set internal standards as they deem appropriate. The terms "should" and "shall" are included to represent the suggested application of the specific guideline.

There is a lot of discussion concerning the terms accreditation, certification, and qualification. It should be noted that SWGDE does not accredit, certify, approve or qualify laboratories or individuals. As discussed above, accreditation is the process by which an agency demonstrates compliance with the process set forth by the accreditation body. Certification is a process by which an individual demonstrates accomplishment of a set of requirements set by a certification organization. One example of this is the IACIS

CFCE. Qualification is the approval by an agency for an individual to perform specified duties. To demonstrate these terms, an individual might be certified by IACIS, qualified by their agency to conduct computer forensic examinations within the agency's ASCLD/LAB accredited crime laboratory.

Likewise, there was a great deal of discussion concerning competency and proficiency. Since it is an agency that "qualifies" individuals to perform tasks that might result in liability to the agency, each agency sets its own requirements. This may, or may not, include holding academic degrees or certifications. So, wherever the ASCLD/LAB Manual or the SWGDE Best Practices documents refer to competency, it is left to each agency to determine what set of skills, at what level, are required for a particular position. In the terminology set forth in the ASCLD/LAB Manual, the initial test used by a laboratory to qualify an examiner is referred to as a "competency" test. Tests that are required to determine continued qualification are referred to as "proficiency" tests. It is our hope that the community-at-large will thoughtfully examine the document and consider its benefits to the agencies wishing to create or improve digital evidence programs. We believe that the Quality Assurance issues discussed are important to every organization. In order to avoid confusion, the document title has been changed to:

"Best Practices for Digital Evidence Laboratory Programs".
http://www.fbi.gov/hq/lab/fsc/backissu/july2000/swgroups.htm

http://www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm

http://www.ioce.org/2002/G8%20Proposed%20principles%20for%20forensic%20evidence.pdf

http://www.ascld.org/accreditation.html

http://www.ASCLD-LAB.org/pdf/aslabrevisions.pdf

http://www.ASCLD-LAB.org/aslab08.html