Scientific Working Group on Digital Evidence (SWGDE)
Position on the National Research Council Report to Congress
Strengthening Forensic Science in the United States: A Path Forward

In the National Research Council's February 18, 2009 report to Congress entitled "*Strengthening Forensic Science in the United States: A Path Forward*" (hereafter "*The Report*") the council brought forth a broad overview of the state of forensic science in the United States.

The purpose of SWGDE is to bring together organizations actively engaged in the field of digital and multimedia evidence to ensure quality and consistency throughout the digital forensic community. *The Report* makes several recommendations to further improve the state of forensic science in the United States. This report is a call to action for SWGDE to strengthen the digital evidence discipline. As a result of certain recommendations put forth in *The Report*, SWGDE is compelled to take the following positions:

Recommendation 1: ***The creation of the National Institute of Forensic Science (NIFS)***

The creation of a new federal bureaucracy from the ground up does not happen quickly. Whether or not Congress ultimately decides to create the NIFS, steps can be immediately taken to begin achieving the stated objectives. SWGDE believes that a consortium of existing forensic organizations (the American Academy of Forensic Sciences (AAFS), the International Association for Identification (IAI), etc.), the Scientific Working Groups (SWGs), and laboratories should be convened to begin discussing a national strategy based on the focus areas in this recommendation.

At a minimum, this consortium should establish minimum standards for recognizing new forensic disciplines, establish new analytical methods, and develop a community-wide code of ethics. If funding for improving forensic science is allocated, we recommend developing a competitive process, similar to that used in the Technical Support Working Group (TSWG), to allocate the funds where they can best serve the interests of the community. The driving forces of the consortium should be the development of objective standards and validation of methods by establishing ties to the general scientific research community.

Recommendation 2: ***Standardization of terminology for reporting and testimony.***

SWGDE agrees that standardization of terminology is a vital step in establishing standard practices. To this end, SWGDE in collaboration with the Scientific Working Group on Imaging Technology (SWGIT), has developed and continuously maintains a glossary of terms used within the digital and multimedia disciplines. SWGDE has utilized ASTM International, a recognized standards organization to establish national acceptance of terminology. We also have worked closely with ASCLD/LAB to promote the use of standard terminology.

We have initiated and will continue development of standardized report structures suitable within the discipline. Our published documents currently include templates for standard

operating procedures and validation testing, and list the minimum elements in reports of findings.

The Report discusses the inclusion of measures of uncertainty and estimated probabilities in case reports. It should be noted that most processes regarding digital evidence are discrete in nature and not subject to statistical error. Systematic error is generally identified during validation and accounted for in the standard operating procedures regarding that tool or technique.

Recommendation 3: ***Research to address accuracy, reliability, and validity.***

SWGDE endorses this recommendation. Lacking a large commercial industry that promotes research in the academic community, forensic science is at a competitive disadvantage getting researchers to solve problems relevant to the field. SWGDE identifies issues and needs of the digital forensic community, but has neither the authority nor resources to support the level of research required. SWGDE recognizes trends in the digital and multimedia disciplines and is uniquely positioned to recommend research to funding bodies to address the discipline's needs. For example, we would like to see research funding go toward:

- Validation of digital multimedia tools and compliance with multimedia format specifications
- Studies of sources of cognitive bias in DE exams
- Comprehensive validation of audio authentication methodologies
- Developing strategies and tools to examine dynamically changing technologies

Recommendation 4: ***Removing public labs from administrative control of law enforcement.***

SWGDE does not agree that the removal of labs from law enforcement agencies will free them from the effects of context bias and exigency. Submitters of casework, even if coming from outside an independent laboratory, can always be a source of information leading to bias or pressure to perform quickly. Regardless of the laboratory's funding source or management structure, the customers' desires can be a source of bias for any laboratory or examiner.

We think that the impact of these problems can be minimized by adopting some of the other recommendations contained in this response. Using standardized procedures, documenting deviations from those standards, directed ethics training, and organizational policies that protect the independence of the forensic examiner; all protect against biases that damage results. Removing labs from law enforcement agencies may temporarily relieve the perception of bias, but without checks and balances firmly entrenched within any laboratory, it will not eliminate bias.

Recommendation 5: ***Studying and modeling context bias.***

SWGDE supports the comprehensive study of human observer bias in forensic processes and will modify any of our recommendations and requirements to minimize these errors should

they be found. We also agree that well-formed standard operating procedures can help minimize effects of bias.

Computer forensic examiners must work closely with investigators to effectively search for information on a seized system. This interaction between the examiner and the investigator creates the potential for bias, but as data recovery does not rely on examiner interpretation, it may not offer opportunities for bias to have an effect on the outcome. Having well-formed standard operating procedures for dealing with these situations, as well as a requirement to document deviations from those procedures, affords protection. SWGDE welcomes studies to determine if bias effects are compromising evidence collected under these conditions.

Recommendation 6: ***Collaboration and standards development.***

SWGDE's membership has always included federal, state, and local government, private laboratories, universities and representatives from NIST and ASCLD/LAB actively engaged in the field of digital and multimedia evidence. Our purpose is to bring these entities together to share information, develop best practices and identify education and training requirements.

Accrediting bodies have come to SWGDE for recommendations concerning digital evidence issues. With more funding, we would help facilitate the development of new digital forensic tools and methodologies to keep pace with ever changing technology and ensure that these tools are quickly and properly validated.

Recommendation 7: ***Mandatory accreditation and certification.***

Accreditation:

SWGDE supports accreditation for digital evidence laboratories. However, *mandatory* accreditation using the current process is not feasible for all laboratories (public or private) as it carries a substantial burden on financial and personnel resources, especially for smaller and/or isolated laboratories. At a minimum, SWGDE recommends that all digital evidence laboratories have a written quality management system in place to provide confidence and assurance in the quality of that laboratory's work. By complying with the other quality assurance policies that SWGDE has identified, e.g. administrative and technical reviews; written SOPs that use best practices; and a written quality management system that includes periodic auditing, a laboratory can provide a greater degree of confidence and assurance in its work product.

To have value, any mandatory accreditation *must* hold laboratories accountable to a standard. Forensic laboratory accrediting bodies focus on organizational processes and have used traditional community standards. SWGDE supports uniform standards. Our published recommendations have already been cited multiple times in testimony by non-members as their operational standard. We have worked with ASCLD/LAB for many years to make our recommendations appropriate for use in accreditation. SWGDE has also been recognized by the IOCE as the North American digital evidence policy representative and our practices have been citied by the European Network Forensic Science Institute – Forensic Information Technology Working Group (ENFSI-FITWG) and in publications. We are currently working to have our

best practices adopted by ASTM International as international standards. SWGDE recommends that its published requirements and recommendations be adopted as enforceable standards.

Certification:

SWGDE supports mandatory certification of all digital evidence practitioners. While several certifications exist, it seems unlikely any one certification will ever be all encompassing. Digital evidence is continually changing as is the training and certification related to it. As new operating systems and file systems emerge, so does the training. As the training is created, organizations act quickly to create a method to certify an examiner in the proper method to handle these new types of evidence.

Any mandatory certification must meet the following requirements:

1. The certification must focus on the theory of how digital evidence is created, stored, and recovered and must not be based on specific software or tools.

2. The certification must be based upon a set of core competencies. Certifications that do not spell out their core competencies are likely to become too broad and randomly address the critical issues in this field.

3. There must be recommended training courses and/or a specified number of training hours for the candidate to be eligible for certification. In lieu of the training requirement, a certifying body may consider years of experience in the field as a suitable substitute.

4. The candidate must demonstrate an understanding of the core competencies via a comprehensive written exam.

5. The candidate must demonstrate an understanding of the core competencies via one or more practical examinations. The candidate performing the practical examination(s) must be required to follow SWGDE best practices where appropriate.

6. All candidates for certification must agree to adhere to a strict code of ethics in which the examiner agrees to approach each investigation in a fair and unbiased manner. Violations of the code of ethics will result in a forfeiture of the certification by the certifying body.

7. The certification must require periodic recertification that contains:
   - a practical examination adhering to the core competencies;
   - a specified number of hours of continuing education in the field of digital evidence; and
   - an agreement to continue following the code of ethics.

Recommendation 8: ***Quality assurance and quality control.***

SWGDE agrees with this recommendation and our published documents reflect this. As stated previously, all digital evidence laboratories must employ a written quality assurance system that includes periodic auditing.

Quality assurance depends upon the commitment to excellence by employing techniques to ensure the work product and methodologies are sound and free from error. Several parts to the quality assurance system require more than one person to perform a specified task. A laboratory consisting of a single individual is still responsible for maintaining quality control standards. One way this can be achieved is through partnerships with other labs to leverage quality assurance resources such as proficiency testing, technical reviews, periodic audits, etc.

Recommendation 9: ***Uniform code of ethics.***

To be effective, a code of ethics needs to enforceable. The consortium of forensic organizations mentioned in our response to Recommendation 1 should begin now to synchronize their code of ethics and coordinate a common enforcement scheme. As most forensic practitioners are members of at least one of the organizations in the consortium, a uniform code would then apply to all.

Recommendation 10: ***Developing academic programs in forensic science.***

Academic programs currently exist that benefit digital and multimedia disciplines (e.g., Scholarship for Service, Cyber Corps, NSA Centers of Academic Excellence); however, these programs tend to produce graduates in the Information Assurance field.

Similar programs must be developed with the same rigor to produce graduates who will become certified digital forensic examiners with minimal additional training. For example, education in audio related fields is largely driven by the telecommunications and entertainment industries. The convergence of science and engineering interdisciplinary programs towards a forensic focus should be expanded.

Research funding is more critical in digital and multimedia disciplines than any other forensic discipline. These disciplines are driven by technology and logic rather than physics and chemistry. New technology, typically proprietary in nature, emerges daily. As these new technologies emerge, new solutions and techniques are needed to understand and examine evidence. Comprehensive understanding and validated techniques need to move swiftly from the research community to the examiner community. Similarly, continuing education that maintains the proficiency and competency of existing examiners is crucial.

Another concern is the retention of trained personnel in forensic service. Many degree recipients will work for the government as a term of their scholarship agreement to take advantage of federal loan repayment programs. Unfortunately, they are often recruited to non-forensic science positions in the private sector where the financial benefits are greater once their

obligation is fulfilled. Other enticements such as graduate degrees or post-graduate opportunities could be supported to improve retention, raising the level of competence.

Recommendations 11 and 12:

These recommendations do not apply to SWGDE.

Recommendation 13: *Homeland security*.

SWGDE has a major stake in homeland security investigations. The subway and bus bombings in the United Kingdom, the Madrid train bombing, the Mumbai bombing, and the 9/11 attacks on the United States all contained large amounts of digital evidence such as video surveillance documenting the movements of terrorists, cell phone intercepts and records of terrorist communications, and GPS data used for covert command and control. Crimes such as identity theft and cyber security breaches are having more dramatic impacts each year. SWGDE is willing to ensure that homeland security applications of digital evidence examination are developed to the highest standards while preserving the evidentiary value of information collected.