Council of the
INSPECTORS GENERAL
on INTEGRITY and EFFICIENCY

QUALITY STANDARDS FOR DIGITAL FORENSICS

November 20, 2012

TABLE OF CONTENTS

PREFACE .... **ii**

MANAGEMENT STANDARDS **1**

A. DIGITAL FORENSIC CAPABILITY 1

B. QUALITY MANAGEMENT 2

PERSONNEL STANDARDS **3**

A. QUALIFICATIONS 3

B. PROFICIENCY 5

PREFACE

The standards and principles contained in the Quality Standards for Digital Forensics (QSDF) provide a framework for performing high-quality digital forensics in support of investigations conducted by an Office of Inspector General (OIG) affiliated with the Council of the Inspectors General on Integrity and Efficiency (CIGIE). These standards also have value to personnel and organizations providing digital forensic support to audits, inspections, or other OIG work.

For the purpose of these standards, digital forensics is defined as a subset of the forensic discipline known as Digital and Multimedia Evidence, which involves the scientific examination, analysis, and evaluation of digital evidence in legal matters. It includes acquiring and preserving digital evidence in any form, as well as analyzing computers, personal digital assistants, tablets, cellular telephones, and other digital devices with a processor. Digital forensics does not include image (photo) analysis, video analysis, forensic audio, or data mining. It also does not include the basic, non-forensic review of documents that are in electronic format (for example, simply reading an electronic document is not digital forensics).

The standards outlined here are relevant to all aspects of the digital forensic process, including acquisition, examination, analysis, and reporting. Recognizing that members of the OIG community are widely diverse in their missions, authorities, staffing levels, funding, and daily operations, certain foundational standards are nevertheless needed for any organization performing digital forensics. As such, the QSDF are sufficiently broad to accommodate the diverse environments in which OIGs operate, while still providing minimum standards to ensure quality. Not all OIGs may perform all phases of the digital forensic process; however, it is important that all OIGs have policies pertaining to digital forensics, as most investigations will encounter evidence created by digital devices.

The standards outlined in this document were derived from digital forensics standards and guidance published by the Scientific Working Group on Digital Evidence, the National Institute of Justice, the Department of Justice Computer Crime and Intellectual Property Section, and the National Research Council. The CIGIE Quality Standards for Investigations, Federal Rules of Evidence, and case law were also referenced.

OIGs should incorporate the standards and principles outlined here into an operations manual or handbook. This should be accomplished in accordance with the OIG's particular mission, unique circumstances, and respective department or agency requirements. OIGs are encouraged to monitor changes in the laws, regulations, and industry best practices and revise their policies as necessary, pending future releases of the QSDF. If the QSDF are found to be inconsistent with laws, rules, regulations, or other pertinent official pronouncements, the latter take precedence.

This document outlines standards in two areas: management and personnel. Management standards pertain to the organization and the environment in which digital forensics are performed. Personnel standards pertain to the standards applied to the individual conducting digital forensics.

QUALITY STANDARDS FOR
DIGITAL FORENSICS

MANAGEMENT STANDARDS

Management standards apply to the organizational environment in which digital forensics are performed. It includes the policies and procedures that create the organizational environment and processes that personnel follow when performing digital forensics. The two management standards address digital forensic capability and quality management.

A. Digital Forensic Capability

> *All organizations conducting investigations that may require the use of digital forensics must ensure the investigations can be supported by forensically sound and legally sufficient digital forensic examinations.*

This standard places on the organization the responsibility for ensuring it has policies and procedures to ensure digital forensics can support its investigations, when appropriate. This standard does not require that every organization be capable of performing digital forensics. If an organization does not have the capability to forensically acquire or analyze digital evidence, it should have policy indicating how it will handle the situation when these capabilities are needed.

Guidelines

Digital devices are prolific in today's society. People routinely use them to communicate with others (through email, chat, etc.), create documents, access and enter data online, and store a wide variety of information from pictures to written documents. Virtually all investigations will involve relevant digital data processed or stored by these devices. Because this digital data may contain both incriminating and exculpatory evidence, it is imperative that every organization performing investigations be able to conduct digital forensics or have the support of another capable entity. Therefore, every organization must have a policy on how digital media will be acquired and processed. If the organization conducts forensic functions internally, it must have additional policies or procedures guiding how personnel will perform those functions. If the organization is supported by another entity, then the organization must ensure the entity meets the standards outlined in this document. An organization can meet this requirement by obtaining support from another OIG held to these standards or an agency accredited according to International Organization for Standardization (ISO) 17025, or by obtaining documentation from the supporting entity sufficient to demonstrate compliance with these standards.

Organizations performing specific digital forensic tasks must adhere to the following basic standards.

Legal Authority—Before any forensic examination, examiners must ensure they have the legal authority (such as a search warrant or consent) to search through the digital data. Because of how data is stored on computers and other digital devices, the large volume of data usually present, and the complexities involved with searching the data, an organization is frequently authorized to seize all the digital data for searching at a later date in a controlled laboratory environment. The subsequent search must be within the bounds of the consent or comply with the search warrant or other authority. Therefore, each forensic examiner assigned to conduct an analysis must review the pertinent search warrant, consent, or other document authorizing the examination pertaining to the evidence to be examined. Forensic examiners should work with the prosecutor or organization's counsel to resolve any questions about the authority to conduct the examination.

Integrity of Evidence—Digital data can be easily altered, and environmental conditions (such as strong magnetic fields) can affect the integrity of data on certain storage mediums. Organizations must carefully ensure data are not unintentionally altered during or after the acquisition. Organizations can ensure data are not unintentionally altered during acquisition by performing appropriate validation testing of acquisition tools and by using appropriate procedures. Organizations must ensure personnel handle and store data in a manner that precludes the inadvertent alteration or destruction of evidence by human action or environmental conditions.

Forensic Documentation—Organizations must properly document forensic activities and results to meet the requestor's needs and allow for the evaluation of forensic activities with these standards. Forensic reports and related documentation should include, at a minimum, the following:

- Identity of the reporting organization
- Case identifier or submission number
- Identity of the submitter
- Relevant dates for forensic work, to include date of report
- Descriptive list of the evidence examined
- Examination requested
- Description of the examination
- Name and signature (handwritten or digital) of the examiner
- Results, conclusions, and derived items

B. Quality Management

> *Organizations conducting digital forensic examinations must implement a quality management system to govern digital forensic methodologies and work products.*

This standard places on the organization the responsibility for ensuring the organization has quality practices and procedures in place sufficient to provide confidence that the results of forensic examinations are of high quality.

Guidelines

Digital forensic examinations require an examiner to apply a wide range of techniques to retrieve data, and frequently examiners must interpret data to offer an expert opinion on what the data mean. These opinions can affect the outcomes of investigations, prosecutions, or other remedies. It is therefore essential that organizations have a management system to engender confidence in the quality of forensic work performed. The quality management system is the consolidation of practices and procedures used to ensure the quality of the work and products that the organization produces.

Administrative Review—All digital forensic examination reports must be administratively reviewed for consistency with agency policy and for editorial correctness.

Technical Review—At least 10 percent of final digital forensic examination reports must be technically reviewed by another qualified digital forensic examiner (peer reviewed) before the reports are published.

The reviewing examiner may be from the same or a different organization. The purpose of the technical review is to ensure the following:

- The report is clear and understandable.
- The procedures performed were adequately documented and forensically sound.
- The exam documentation was sufficiently detailed to enable reproduction of the results.
- The interpretations and conclusions of the examiner were reasonable, supported by the examination documentation, and scientifically valid.

Validation Testing—Acquiring digital data for forensic examination is a critical phase of the forensic process. Forensic personnel will often have only one opportunity to obtain the data, and using untested tools could unintentionally alter the data. To the extent possible, organizations should ensure the tools they use to acquire digital evidence are validated to operate as intended and accurately acquire the data. The validation testing may be performed by the organization or other reputable entity (for example, another digital forensic laboratory). The organization performing the validation test must document the test, including the requirements that were tested, the expected results, and the actual results of the testing. To comply with this standard, the organization must be able to produce the report if requested.

Review of Quality System—An organization should review its quality management system at least once every 3 years to ensure the system is meeting the quality needs of the organization.

PERSONNEL STANDARDS

Personnel standards apply to all the personnel performing digital forensic tasks in the organization. The personnel standards address qualifications and proficiency. For the purposes of these standards, digital forensic personnel are categorized as one of the following:

- Examiners (Analysts)—Personnel who examine, analyze, or recover digital evidence. An examiner may also be responsible for collecting digital evidence.
- Specialist—Personnel who collect or prepare digital evidence for examination and analysis.

A. Qualifications

> *Personnel assigned to perform digital forensic activities must possess technical competency for the tasks they are assigned.*

This standard places on the organization the responsibility for ensuring that individual forensic tasks are performed only by personnel who have the knowledge and proven technical competency required to perform those tasks.

Guidelines

Digital forensics support to investigations can involve a wide range of activities, from simply extracting logical files to recovering and interpreting fragments of digital data to determine the activities that occurred on the digital device. The digital evidence to be analyzed can be obtained from a variety of electronic hardware running different computer or mobile operating systems and storing data in different formats.

Organizations should establish criteria to be used in recruiting and selecting the best qualified applicants to perform digital forensics. At a minimum, factors to consider in selecting personnel to perform digital forensics should include education, experience, character, ability to understand technical concepts, and the ability to solve problems. Each of these factors may be controlled by legislation, regulation, or agency needs. Organizations should review these criteria to ensure they assist in providing the best qualified candidates. Once the organization selects personnel to perform forensic duties, the organization must ensure those personnel receive training to obtain the knowledge and skills necessary to perform digital forensics in the organization's environment.

Education—Preferably, all newly appointed personnel performing digital forensics will possess a degree from an accredited 4-year college. The knowledge acquired from higher education will enable the individual to handle complex problems encountered while performing forensics. Higher education also enhances the individual's ability to communicate effectively, both orally and in writing. The individual should also have a demonstrated aptitude for comprehending how computers or networks operate or for understanding technical concepts. This technical aptitude will provide greater assurance of the individual's ability to understand and apply technical concepts involved in computer forensics.

Experience—Depending on the organization's specific needs, the organization may allow candidates to substitute job experience for a college education. Suitable job experience would provide the candidate with pertinent and demonstrable knowledge, skills, and abilities needed to handle complex problems and the ability to understand and clearly communicate technical issues, both orally and in writing.

Character— Each individual performing digital forensics must possess and maintain the highest standards of conduct and ethics, including unimpeachable honesty and integrity. Every citizen is entitled to have confidence in the integrity of Government employees, particularly those who routinely access sensitive information and acquire and analyze digital evidence that may be used to convict someone of a crime. Consequently, OIGs should establish sound hiring policies to adequately screen applicants for digital forensic positions. Processes to consider include, but are not limited to, criminal history checks, queries of commercially available databases, drug testing, personal interviews, previous employment and reference checks, and background investigations.[1]

OIGs should also have policies that require digital forensic personnel to report any arrest, conviction, or other potential misconduct issue that would jeopardize their performance of duties. Such policies may also include requiring these personnel to be subject to periodic criminal history and background checks.

Technical Concepts—Digital forensic personnel must be able to comprehend complex technical concepts. Much of the training for digital forensic examiners involves highly technical information concerning how computers operate and how data are transmitted and stored by computers and other digital devices.

Problem Solving—Digital forensic personnel must be able to analyze a problem and determine courses of action to resolve the problem. Personnel frequently need this skill when troubleshooting different types of computer equipment and when determining methodologies that can resolve forensic challenges.

Entry-Level Training—All personnel performing digital forensics must attend a formal training program for the tasks they will perform. The training must include, as appropriate for the individual's forensic duties:

[1] The Office of Personnel Management (OPM) categorizes background investigations as National Agency Checks with Inquiries (NACI), Moderate Risk Background Investigation (MBI), Background Investigation (BI), and Single Scope Background Investigation (SSBI). Please refer to OPM for further guidance.

- Digital evidence theory
- Preexamination procedures
- Media assessment and analysis
- Data recovery[2]
- Analysis of recovered data[2]
- Documentation and reporting
- Legal considerations and ethics
- Organizational standard operating procedures
- Organizational quality assurance processes

Competency—Personnel performing digital forensics must demonstrate they are competent to perform digital forensics before performing independent work. Most formal digital forensic training programs include both a written and a practical exam at the end of the course, and this examination is sufficient to demonstrate competency. Likewise, an agency may choose to accept a formal certification in digital or computer forensics achieved through testing as a demonstration of competency.

B. Proficiency

> *Personnel conducting digital forensics must maintain proficiency to conduct the tasks they are assigned.*

This standard places on the organization the responsibility for ensuring that personnel performing digital forensic tasks are provided continuing education and training to maintain the necessary skills despite changing technologies. The organization also has the responsibility to periodically evaluate personnel proficiency.

Guidelines

The ways in which digital devices process and store data change regularly as hardware and software are upgraded. Additionally, tools and techniques for analyzing digital data are continually evolving. Digital forensic examiners must keep abreast of the latest changes to ensure they are able to properly conduct forensic examinations.

Continuing Education—All personnel performing digital forensics must receive continuing education in digital forensics, information technology, or related topics. During every 3-year period, examiners must receive a minimum of 60 hours of training, and specialists must receive a minimum of 24 hours. In addition to increasing an individual's competency, this training is critical to ensure forensic personnel are informed of changes that affect digital forensics. This training can be accomplished through a variety of methods, including but not limited to formal training classes, conferences, online training, in-house training or practice, and approved self-study.

Proficiency Testing—Personnel performing digital forensics must demonstrate they continue to maintain their proficiency to perform digital forensics. Forensic personnel must pass a practical proficiency test once every 3 years. An agency may choose to have forensic personnel complete this requirement through a test offered by an external proficiency test provider, a test needed to maintain a digital forensics certification, or a test developed in-house or by another digital forensic organization. Personnel are not

[2] Not required for specialists; however, knowledge in this area can aid in collecting and preparing digital evidence.

allowed to demonstrate their proficiency by taking the same test they developed or graded. Agencies should give due consideration when recording the successful completion of proficiency tests, recognizing records may be introduced as part of future litigation involving the individuals' qualifications.