Council of the
INSPECTORS GENERAL
on INTEGRITY and EFFICIENCY

# QUALITY STANDARDS FOR DIGITAL FORENSICS

June 18, 2019

# Message from the Chairpersons of the CIGIE Information Technology and Investigations Committees

According to Section 11 of the Inspector General Act of 1978 (5 U.S.C. app. 3), as amended, the Council of the Inspectors General on Integrity and Efficiency (CIGIE) shall address integrity, economy, and effectiveness issues that transcend individual Government agencies and increase the professionalism and effectiveness of personnel by developing policies, standards, and approaches to aid in the establishment of a well-trained and highly skilled workforce in the Offices of Inspectors General. As such, the CIGIE Information Technology and Investigations Committees collaborated to produce these Quality Standards for Digital Forensics (QSDF).

As dependence on computers, tablets, and mobile devices increases and the cost of digital storage decreases, the amount of electronically stored information continues to increase rapidly. If accessed correctly and legally, this digital information can be extremely valuable for investigative use. As with all disciplines and specialties, the digital forensics community has matured and the technologies used have evolved, warranting a review and update of the first QSDF issued on November 20, 2012.

The standards and principles contained in this updated 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 CIGIE. These standards also have value to personnel and organizations providing digital forensic support for audits, inspections, or other OIG work.

Although members of the OIG community are widely diverse in their missions, authorities, staffing levels, funding, and day-to-day operations, certain foundational standards apply to any investigative organization. As such, the QSDF outlined in this document are comprehensive, relevant, and sufficiently broad to accommodate a full range of digital forensic support for OIG criminal, civil, and administrative investigations across the CIGIE membership.

We wish to thank the members of the Information Technology Investigations Subcommittee who incorporated into this update quality management principles and practices that are essential to ensuring quality digital forensic products. Their tremendous efforts in balancing quality measures with the impact on both large and small OIGs and coordinating these changes with all the CIGIE OIGs has resulted in these standards that will help ensure OIGs have quality digital forensics services available to support their investigative and other missions.

Tammy L. Whitcomb
Chair, Information Technology Committee

Michael J. Missal
Chair, Investigations Committee

## TABLE OF CONTENTS

# PREFACE

The Quality Standards for Digital Forensics are written to address the processes and specialized techniques for gathering, retaining, and analyzing electronically stored information (ESI), and reporting the resulting conclusions for investigative purposes. The standards are not intended to address the specialized investigative analysis of photographic images, video, or audio. The standards also do not apply to the basic, non-forensic review of electronic documents or user-accessible file metadata, extraction of text from log files, and data mining. Likewise, the systematic extraction/copy of existing data files or records consistent with Federal Rules of Evidence 902(14) is not subject to these standards since it does not involve a forensic expert interpreting data or drawing conclusions or using forensic tools or techniques to retrieve the data.

Instead, these standards apply only to the acquisition, examination, and analysis of ESI, and the associated reporting, that requires specialized training, equipment, or software to ensure that the results and conclusions are accurate and admissible in legal proceedings. Digital forensics is not limited to ESI stored on traditional computers, but includes the acquisition, preservation, and analysis of ESI on tablets, mobile devices, and other digital devices with a processor.

Digital investigation of a device or ESI can be an iterative and cumulative process that can include multiple investigative and analytical steps and may also result in multiple reports of different scope on the same evidence. Forensic analysis and reporting is only one part of the investigation of digital devices or ESI. 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 ESI. When an OIG requires capabilities or skills beyond its abilities, it is encouraged to seek the assistance of other qualified OIGs.

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 qualifications and proficiency of individuals conducting digital forensics.

OIGs must incorporate the standards and principles outlined here into written policies and procedures appropriate to their specific operating environment. 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. OIGs must also maintain documentation sufficient to demonstrate conformity with these standards during quality assessment reviews. If an OIG chooses to obtain a formal International Organization for Standardization accreditation for its digital forensic work, then the proof of accreditation is adequate to demonstrate conformity for quality assessment reviews.

# QUALITY STANDARDS FOR DIGITAL FORENSICS

# I. MANAGEMENT STANDARDS

Management standards apply to the organizational environment in which digital forensics are performed. It includes the requisite written 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 each organization conducting investigations that may result in adjudicative proceedings the responsibility for having policies and procedures to ensure digital forensics can be used to support its investigations, when appropriate and consistent with the guidelines below. 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 ESI, it must have policy indicating how it will handle the situation when these capabilities are required. If the organization conducts forensic functions internally, it must have additional policies or procedures implementing the standards outlined in this document in the environment of that organization.

**Guidelines**

1. **General**—Digital devices are prolific in today's society. People routinely use them to communicate with others, create documents, access and enter data online, and store a wide variety of information. The majority of investigations will involve relevant ESI processed or stored by these devices, although the volume of the ESI and requirements of the analysis may vary. Because this ESI 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.

2. **Legal Authority**—Before any forensic examination, staff must ensure they have the legal authority (such as a search warrant or consent) to search through the digital device or ESI. Because of how data is stored on computers and other digital devices, the large volume of ESI usually present, and the complexities involved with searching ESI, an organization is frequently authorized to seize all the ESI 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.

3. **Integrity of Evidence**—ESI can be easily altered and environmental conditions (such as strong magnetic fields) can affect the integrity of data on certain storage mediums. Organizations must ensure ESI is not unintentionally altered during or after the acquisition. Organizations can ensure ESI is 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 ESI in a manner that precludes the inadvertent alteration or destruction of evidence by human action or environmental conditions. The chain of custody for all digital evidence must be maintained, consistent with the organization's evidence policy and the requirements outlined in the CIGIE *Quality Standards for Investigations*.

4. **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. A digital forensic examination report must be written any time an examiner provides expert opinion, interprets digital data, draws conclusions, or uses specialized digital forensic knowledge or techniques to recover/reconstruct information. Digital media extraction summaries or validated, automated software reports that simply identify the existence of digital data can precede digital forensic examination reports, but in isolation, are not in themselves sufficient for conclusions or opinions that should be rendered in digital forensic examination reports. Digital forensic examination reports or summaries of extractions or other activities, together with associated documentation in the official file, should include, at a minimum, the following:

- Identity of the reporting organization
- Case identifier or submission number
- Identity of the submitter
- Relevant dates, including report or summary date
- Descriptive list of the evidence examined
- Examination or other actions requested
- Description of the examination or other actions, as appropriate
- Name and signature (handwritten or digital) of the examiner
- Results, conclusions, and derived items, as appropriate
- Contemporaneous work notes (or detailed automated logs)

5. **External Forensic Support**—Organizations lacking necessary digital forensic capabilities or expertise may enter into a contract or formal agreement with external entities such as another OIG, government agency, or a private contractor, to provide these capabilities. Organizations should ensure that the supporting entity operates consistent with the guidelines set forth in this document. An organization can meet this requirement by obtaining support from another OIG that has passed a Quality Assessment Review using these standards or from an entity accredited to perform digital evidence examination in accordance with applicable International Organization for Standardization standards. Verification that the entity meets these standards can also be obtained by reviewing documentation from the supporting entity sufficient to demonstrate compliance. Alternatively, the organization may document an assessment of the external entity's historic performance in producing quality work products. This assessment can be accomplished by reviewing the external entity's demonstrated specialized investigative and judicial experience and/or use by other Federal law enforcement or the U.S. Department of Justice.

## 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 having policies and procedures implementing quality management practices sufficient to provide confidence that the results of forensic examinations are of high quality, consistent with the guidelines below.

## Guidelines

1. **General**—Digital forensic examinations, in contrast to basic file or record extraction from ESI, may require the application of a wide range of techniques to retrieve data, or the examiner may need to interpret the data or offer an opinion on what the data mean. These opinions may affect the outcomes of investigations, prosecutions, or other remedies. It is therefore essential that organizations have a documented quality management system to engender confidence in the quality of forensic work performed. The quality management system is the consolidation of policies, practices, and procedures used to ensure the quality of the work and products that the organization produces.

2. **Administrative Review**—All digital forensic examination reports must be administratively reviewed by another individual for consistency with organizational policy.

3. **Technical Review**—At least 50 percent of final digital forensic examination reports must be technically reviewed by another qualified digital forensic examiner (peer reviewed) before the reports are published. Beginning in fiscal year 2024, all final digital forensic examination reports must be technically reviewed. 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; and
- The interpretations and conclusions of the examiner were reasonable, supported by the examination documentation, and scientifically valid.

4. **Validation Testing**—Acquiring ESI for forensic examination is a critical phase of the forensic process. Forensic personnel will often have only one opportunity to obtain the ESI, and using untested tools could unintentionally alter the ESI. Validation is an evaluation to determine if a hardware or software tool, technique or procedure functions correctly and as intended. To the extent possible, organizations should ensure the tools they use to acquire ESI are validated to operate as intended and accurately acquire the ESI. 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.

5. **Verification of Findings**—The organization should have a policy concerning the verification of significant findings when validated or generally accepted examination tools are not used. Cross-verification can be accomplished through the use of a secondary tool or through manual interpretation of the data.

6. **Document Control**—Policies, forms, and other standard internal documents used for digital forensics should be centrally controlled and made readily accessible to prevent the unintended use of obsolete versions.

7. **Testimony Monitoring**—Each organization must assess all expert testimony given by its employees in a criminal proceeding that supports digital forensic work performed by the individual providing testimony. The assessment can be accomplished by direct observation, transcript review, or video/audio recording review. The assessment must indicate if the testimony was satisfactory or unsatisfactory, and should assess whether the examiner's:

- Testimonial opinions, conclusions, and statements regarding the underlying case-specific facts or data were properly qualified and did not exceed the limitations of the method performed or the discipline in question; and
- Conclusions are in conformity with the directives of any applicable approved Uniform Language for Testimony and Reports document.

The satisfactory or unsatisfactory evaluation of the testimony must be in writing; however, any feedback should be provided verbally. If testimony is found to be unsatisfactory, the prosecuting attorney must be notified of the circumstances.

8. **Corrective Actions**—Deficiencies, failures, or other events that potentially negatively impact the quality of the organization's forensic products must be documented and corrective action taken. Documentation should include a description of the deficiency, failure, or event and the actions taken to address the issue and prevent reoccurrence.

9. **Review of Quality Management System**—Each organization must review its own quality management system at least once every fiscal year. The purpose of the quality management system review is to ensure the system is meeting the quality needs of the organization by addressing the following areas, where applicable:

- All policies and procedures remain current and consistent with community best practices;
- All corrective measures taken or any preventative actions instituted have been properly documented and addressed;
- Significant customer complaints received must be reviewed and addressed;
- Formal internal or external recommendations for improvement must be considered and, as appropriate, acted upon; and
- The documented results of the annual review must include the matters reviewed; any identified issues or areas for improvement; and recommendations, plans, or measures implemented or planned for implementation. Additionally, the organization should ensure that any measures or actions planned or recommended are implemented in a timely manner.

# II. PERSONNEL STANDARDS

Personnel standards apply to all 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 ESI. An examiner may also be responsible for collecting ESI.
- Specialist—Personnel who collect or prepare ESI for examination and analysis by an examiner.

## 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 individual forensic tasks are performed only by personnel who have the knowledge and proven technical competency required to perform those tasks, consistent with the guidelines below.

## Guidelines

Digital forensics support to investigations can involve a wide range of activities, from simply extracting logical files to recovering and interpreting fragments of ESI to determining the activities that occurred on the digital device. The ESI 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.

1. **General**—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 organizational 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.

2. **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 and understand technical concepts. This technical aptitude will provide greater assurance of the individual's ability to understand and apply technical concepts involved in computer forensics.

3. **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.

4. **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 ESI that may be used to convict someone of a crime. Consequently, organizations 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.

Organizations 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 be subject to periodic criminal history and background checks.

5. **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.

6. **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.

7. **Entry-Level Training**—All personnel performing digital forensics must attend a formal training program for the tasks they will perform. Organizations may consider the guidance contained in the National Initiative for Cybersecurity Education Cybersecurity Workforce Framework, but the training must include, as appropriate for the individual's forensic duties:

- Digital evidence theory
- Preexamination procedures
- Media assessment and analysis
- Acquisition of digital evidence
- Data recovery[1]
- Analysis of recovered data[1]
- Documentation and reporting
- Legal considerations and ethics
- Organizational standard operating procedures
- Organizational quality assurance processes

8. **Competency**—Personnel performing digital forensics must demonstrate they are competent to perform digital forensics before performing independent work. Ideally this occurs under mentorship of an experienced examiner who certifies to the examiner's competency. 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 organization 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 and record personnel proficiency.

### Guidelines

1. **General**—The manner in which digital devices process and store data changes rapidly as hardware and software are updated, technologies evolve, and new digital devices are developed. 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.

2. **Continuing Education**—All personnel performing digital forensics must receive continuing education in digital forensics, expert testimony, information technology, or related topics. During every 3-year period, examiners must receive a minimum of 120 hours of training, and specialists must receive a minimum of 60 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, as appropriate to the operating environment of each

[1] Not required for specialists; however, knowledge in this area can aid in collecting and preparing ESI.

organization, including but not limited to formal training classes, conferences, online training, in-house training or practice, and documented, approved self-study.

3. **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 organization 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 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.