APPENDIX C-2

Questionnaire for Review of Conformity with Quality Standards for Investigations (Digital Forensics)

PURPOSE. Appendix C-2 is used to assess an organization’s conformity with computer forensic standards. Incorporation of Appendix C-2 (a review of computer forensics activities) is not mandatory. It is an “opt-in” feature of a peer review, until it becomes mandatory in October 2014; however, early adoption is encouraged. If the OIG organization being reviewed has computer forensic capability, it may, prior to commencement of the review, opt to have its computer forensics activities reviewed. If an organization does opt in, the results of the computer forensics review will be included in the overall assessment of the OIG organization. Note that regardless of whether or not an organization opts in, the investigative aspects of computer-related cases (planning, execution, and reporting) will be reviewed relative to the Quality Standards for Investigations (QSI)[1] if such cases are part of the sample case file selection. Appendix C-2 involves an additional review step—focusing on the technical aspects of computer forensics operations. If the OIG organization conducting the peer review does not have in-house personnel with computer forensic capability to conduct the review, it may seek assistance from other Council of the Inspectors General on Integrity and Efficiency (CIGIE) organizations.

Review Step	N/A	PHASE 1 Policy/ Procedure		PHASE 2 Consistent Practice		Reviewed Agency Policy/Manual Reference	QSI Guideline Reference	Comments
		Yes	No	Yes	No			
E. DIGITAL FORENSIC MANAGEMENT - The Standards for the management of digital forensic activities supporting the organization as well as the standards for management of any digital forensic activity performed within the organization.								
48. Does the organization have policy and procedures concerning acquisitions and analysis of digital media?		□	□	□	□			
49. Does the organization have a quality management system to govern the digital forensic methodologies and work products?	□	□	□	□	□			
50. Does the organization periodically review its quality management system, but not to exceed once every three years?	□	□	□	□	□			
51. Do the organization’s examiners ensure sufficient legal authority exists to conduct acquisitions and examinations?	□	□	□	□	□			
52. Does the organization maintain documentation of results from validation testing on tools used in the acquisition of digital evidence?	□	□	□	□	□			
53. Is digital evidence acquired and maintained in a manner that protects and preserves the integrity of the evidence?	□	□	□	□	□			

Questionnaire for Review of Conformity with
Quality Standards for Investigations (Digital Forensics)

Review Step	N/A	**PHASE 1** Policy/ Procedure		**PHASE 2** Consistent Practice		Reviewed Agency Policy/Manual Reference	QSI Guideline Reference	Comments
		Yes	No	Yes	No			
54. Are 10% of final forensic examination reports reviewed by a qualified digital forensic examiner, and are 100% of final forensic examination reports administratively reviewed prior to publication?	□	□	□	□	□			
55. Do final forensic reports or documentation contain, at a minimum, the following: • Identity of reporting organization • Case identifier or submission number • Identity of the submitter • Date of receipt and date of report • Descriptive list of evidence examined • Examination requested • Description of examination • Identity and signature of the examiner • Results/conclusions/derived items	□	□	□	□	□			
56. Is the documentation (including notes) of completed digital forensic analysis sufficiently detailed to evaluate the analysis and enable reproduction of results?	□	□	□	□	□			

F. DIGITAL FORENSIC PERSONNEL - The Standards for the organization's personnel who are assigned duties to collect, preserve, and analyze electronic evidence for potential judicial proceedings.								
57. Have the personnel performing a digital forensics action been trained for that duty? Did the training include, as appropriate for the individual's forensic duties: • Digital evidence theory • Pre-examination procedures • Media assessment and analysis • Data recovery • Analysis of recovered data • Documentation and reporting • Legal and ethics • Organizational standard operating procedures • Organizational quality assurance process	□	□	□	□	□			
58. In order to maintain their technical skills and competencies, do digital forensic personnel receive a minimum of 60 hours of training every three years in digital forensics, information technology, or related topics?	□	□	□	□	□			
59. Do digital forensic personnel pass a competency exam prior to initially conducting independent forensic work (may be part of training)?	□	□	□	□	□			
60. Do digital forensic personnel pass a proficiency exam once every three years to demonstrate continued proficiency?	□	□	□	□	□			