Organization of

OSAC

Scientific Area Committees

Priority Action Report

Digital Evidence

Digital / Multimedia

James Darnell

2/1/2016

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

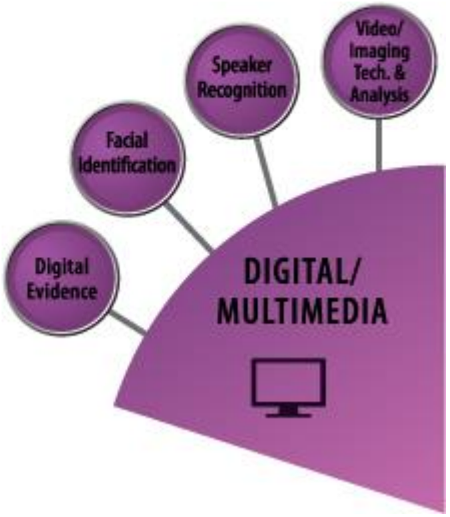
Subcommittee Leadership

Position	Name	Organization	Term	Email
Chair	James Darnell	U.S. Secret Service	2	james.darnell@usss.dhs.gov
Vice Chair	Sam Brothers	Customs and Border Protection	3	sam.i.brothers@cbd.dhs.gov
Executive Secretary	Andrew Neal	TransPerfect Legal Solutions	2	aneal@transperfect.com

Subcommittee Members

#	Name	Organization	Term	Email
1	Bill Eber	Department of Defense	2	buzzbill@gmail.com
2	Mark Phillips	Johnson County Sheriffs Office	4	mark.phillips@jocogov.org
3	Mary Horvath	Federal Bureau of Investigation	4	mary.horvath@ic.fbi.gov
4	Ryan Pittman	NASA, OIG	4	ryan.d.pittman@nasa.gov
5	Sabrina Feve	U.S. Atty Office, San Diego, CA	3	sabrina.feve@usdoj.gov
6	Ovie Carroll	Department of Justice	4	ovie.carroll@usdoj.gov
7	Dave Hallimore	Houston Forensic Science Center	4	forensicaudio@gmail.com
8	Jeff Taylor	Arkansas State Crime Laboratory	4	jeff.taylor@crimelab.arkansas.gov
9	Jim Lyle	NIST	3	Jlyle@nist.gov
10	Marcus Rogers	Purdue University	3	rogersmk@purdue.edu
11	Joshua Brunty	Marshall University	4	josh.brunty@marshall.edu
12	James Adam Holland	Wal-Mart Stores, Inc.	3	James.A.Holland@walmart.com
13	David Papagiris	Iron Mountain	2	David.Papargiris@ironmountain.com
14	Joseph Cassilly	State's Atty, Harford County, MD	2	jicassilly@harfordcountymd.gov
15	Daren Ford	Weld County Sheriff's Office	2	dford@co.weld.co.us
16	Paul Reedy	Washington D.C. Consolidated Lab	3	paul.reedy@dc.gov
17	Steve Wat	Intel Corporation	[illegible]	[illegible]

Discipline Description



The Digital Evidence Subcommittee focuses on standards and guidelines related to information of probative value that is stored or transmitted in binary form.

Summary of Standards/Guidelines Priority Actions

Priority	Working Title of Document
1	Minimum Requirements for Quality Assurance in the Processing of Digital and Multimedia Evidence
2	ASTM E2678-09 Standard Guide for Education and Training in Computer Forensics
3	Forensic Audio Examination, Retrieval, Workflow; new standards derived from SWGDE Best Practices for Forensics Audio (3 new documents)
4	Best Practices for Preservation, Isolation, Acquisition of Mobile and other Embedded Systems; new guidelines derived from NIST 800-101 (3 new documents)

Standards/Guidelines Development Priority 1 Document

Document Title: Minimum Requirements for Quality Assurance in the Processing of Digital and Multimedia Evidence

Scope: This document proposes minimum requirements regarding training/education, examiner certification, examination requirements and lab requirements

Objective/rationale: Describe the minimum requirements necessary to achieve quality assurance in regard to completing digital evidence forensic examinations

Issues/Concerns: The minimum bar may be too high for some to achieve

Task Group Name: Training/Certification
Task Group Chair Name: Andrew Neal
Task Group Chair Contact Information:
aneal@transperfect.com
Date of Last Task Group Meeting: 1/29/2016

Standards/Guidelines Development Priority 1 Document

Key Components of Standard:

- Employment Qualifications
- DME Training / Certification
- Apprenticeship
- Ongoing Training
- Competency and Proficiency Assessments
- Laboratory Standards
- Examination Procedures
- Review
- Reporting

Priority 1: Minimum Requirements for Quality Assurance in the Processing of Digital and Multimedia Evidence

Task Group/Subcommittee Action Plan

Planned Actions	OSAC Process Stage (e.g., SDO 100)	Assignee	Estimated Completion Date
Complete AAFS template and move through SDO Process	SDO 100	Andrew Neal	8/1/2016

Standards/Guidelines Development Priority 2 Document

Document Title: ASTM E2678-09 Standard Guide for Education and Training in Computer Forensics

Scope: This standard is specific to the computer forensics sub discipline of digital and multimedia evidence.

Objective/rationale: Improve and advance computer forensics through the development of model curricula consistent with other forensics science programs

Issues/Concerns: Work with organizations to adopt the model curricula

Task Group Name: Education

Task Group Chair Name: Marcus Rogers

Task Group Chair Contact Information:

rogersmk@purdue.edu

Date of Last Task Group Meeting: 1/29/2016

National Institute of Standards and Technology
U.S. Department of Commerce

Standards/Guidelines Development Priority 2 Document

Key Components of Standard:

- Qualifications
- Core Competencies
- Model curriculum
- Implementation including assessment, faculty, and facilities

Task Group/Subcommittee Action Plan

Planned Actions	OSAC Process Stage (e.g., SDO 100)	Assignee	Estimated Completion Date
Complete registry approval process for existing standard	RA-100	Mark Rogers	4/1/2016

Standards/Guidelines Development Priority 3 Documents

Document Title: Forensic Audio Examination, Retrieval, Workflow, three new standards derived from SWGDE Best Practices for Forensics Audio.

Scope: This document will comment on only those matters that may effect the audio forensic examination process.

Objective/rationale: Provide forensic audio practitioners recommendations for the handling and examination of forensic audio evidence.

Issues/Concerns: None

Task Group Name: Audio
Task Group Chair Name: David Hallimore
Task Group Chair Contact Information:
forensicaudio@gmail.com
Date of Last Task Group Meeting: 1/29/2016

National Institute of Standards and Technology
U.S. Department of Commerce

Standards/Guidelines Development Priority 3 Documents

Key Components of Standard:

- Audio Laboratory Considerations
- Evidence Retrieval
- Receiving Evidence
- Examination
- Administrative and Technical Review

Task Group/Subcommittee Action Plan

Planned Actions	OSAC Process Stage (e.g., SDO 100)	Assignee	Estimated Completion Date
Original document broken into three sections; complete AAFS template for each and submit	SD-100	David Hallimore	8/1/2016

Standards/Guidelines Development Priority 4 Document

Document Title: Best Practices for Preservation, Isolation, Acquisition of Mobile and other Embedded Systems, three new guidelines derived from NIST 800-101

Scope: Organizations should find these documents helpful in establishing their policies and procedures.

Objective/rationale: Help organizations evolve appropriate policies and procedures for dealing with mobile devices and to prepare forensic specialists to conduct forensically sound examinations involving mobile devices.

Issues/Concerns: None

Task Group Name: Mobile Devices

Task Group Chair Name: Steve Watson

Task Group Chair Contact Information:

forensics@stevewatson.net

Date of Last Task Group Meeting: 1/29/2016

Standards/Guidelines Development Priority 4 Document

Key Components of Standard:

- Forensic tools and classification system
- Preservation
- Acquisition
- Examination and analysis
- Reporting

Task Group/Subcommittee Action Plan

Planned Actions	OSAC Process Stage (e.g., SDO 100)	Assignee	Estimated Completion Date
Original document broken into three sections; complete AAFS template for each and submit	SD-100	Steve Watson	8/1/2016

Summary of Standards/Guidelines Priority Actions

Priority	Working Title of Document
1	Minimum Requirements for Quality Assurance in the Processing of Digital and Multimedia Evidence
2	ASTM E2678-09 Standard Guide for Education and Training in Computer Forensics
3	Forensic Audio Examination, Retrieval, Workflow; new standards derived from SWGDE Best Practices for Forensics Audio (3 new documents)
4	Best Practices for Preservation, Isolation, Acquisition of Mobile and other Embedded Systems; new guidelines derived from NIST 800-101 (3 new documents)

Standards/Guidelines Reviewed For Technical Merit

Title	Developing Organization	Status*	OSAC Process Stage (e.g., RA 100)
Minimum Requirements for Quality Assurance in the Processing of Digital and Multimedia Evidence	AAFS	Complete AAFS template and move through SDO Process	SD-100
ASTM E2678-09 Standard Guide for Education and Training in Computer Forensics	ASTM	Complete registry approval process for existing standard	RA-100

Standards/Guidelines Reviewed For Technical Merit

Title	Developing Organization	Status*	OSAC Process Stage (e.g., RA 100)
Forensic Audio Examination, Retrieval, Workflow; new standards derived from SWGDE Best Practices for Forensics Audio (3 new documents)	AAFS	Original document broken into three sections; complete AAFS template for each and submit	SD-100

Standards/Guidelines Reviewed For Technical Merit

Title	Developing Organization	Status*	OSAC Process Stage (e.g., RA 100)
Best Practices for Preservation, Isolation, Acquisition of Mobile and other Embedded Systems; new guidelines derived from NIST 800-101 (3 new documents)	AAFS	Original document broken into three sections; complete AAFS template for each and submit	SD-100

Research Gaps Identified

- The digital evidence community uses file hashing as a means to determine if files, be they image or user, are a match. A research project was requested that examines the underlying scientific principles of using the file hash algorithms in such a manner

Additional Items of Interest

- Short Term
  - SDO and tech merit forms completed
  - TGs working into appropriate SDO templates

- Long Term
  - Lab accreditation
    - Mandatory; Minimum requirements; Possibly addessed in a DE specific supplemental
  - Method / process validation
  - Effects of long term exposure of examiners to questionable material

Organization of OSAC Scientific Area Committees

Priority Action Report

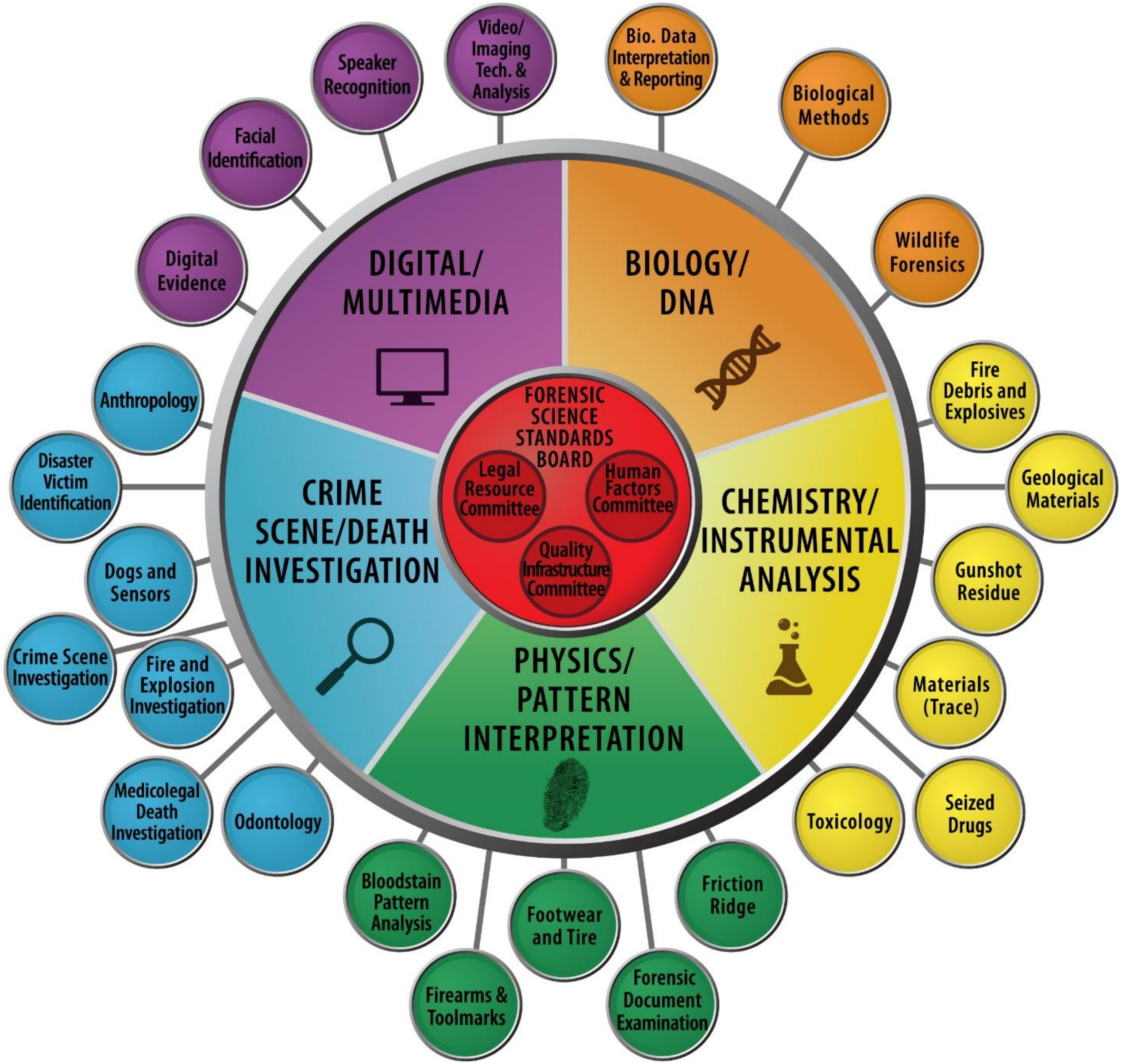
Digital Evidence

Digital / Multimedia

James Darnell

2/1/2016

NIST
National Institute of Standards and Technology
U.S. Department of Commerce


FORENSIC SCIENCE STANDARDS BOARD
Legal Resource Committee
Human Factors Committee
Quality Infrastructure Committee
DIGITAL/ MULTIMEDIA
BIOLOGY/ DNA
CHEMISTRY/ INSTRUMENTAL ANALYSIS
PHYSICS/ PATTERN INTERPRETATION
CRIME SCENE/DEATH INVESTIGATION
Digital Evidence
Facial Identification
Speaker Recognition
Video/ Imaging Tech. & Analysis
Bio. Data Interpretation & Reporting
Biological Methods
Wildlife Forensics
Fire Debris and Explosives
Geological Materials
Gunshot Residue
Materials (Trace)
Seized Drugs
Toxicology
Friction Ridge
Forensic Document Examination
Footwear and Tire
Firearms & Toolmarks
Bloodstain Pattern Analysis
Odontology
Medicolegal Death Investigation
Fire and Explosion Investigation
Crime Scene Investigation
Dogs and Sensors
Disaster Victim Identification
Anthropology

Organization of OSAC Scientific Area Committees

National Institute of Standards and Technology
U.S. Department of Commerce