International Association of Chiefs of Police (IACP)

State, Local, Tribal, & Territorial Digital Forensics…

Addressing the Needs of Law Enforcement

Serving the Leaders of Today, Developing the Leaders of Tomorrow

IACP Computer Crime and Digital Evidence Committee

- Collaborate with the US Partners;
  - BJA, NW3C, SEARCH, NIJ, FLETC, NIST, IJIS Institute, Cyber Shield Alliance, HTCIA
  - US FSLTT LEAs
  - Relevant Private Sector Stakeholders
- Collaborate with International partners;
  - EC3,
  - IGCI,
  - CACP, ACPO/NCCC, etc.
  - International LEAs
- Focus: Cybercrime Investigation, Digital Evidence, and LEA Cybersecurity

CCDE Background:

- NIJ Digital Forensic Research **(2001-2002)**
- Computer Crime & Digital Evidence Committee **(2010)**
- Law Enforcement Cyber Center **(2015)**
- IACP Relevant Research/Awareness **(2013-2016)**
  - LEA Executive Cybercrime and Digital Evidence Research
  - Partnering with IJIS Institute Digital Evidence Task Force
  - NW3C Polling of Practitioners

Digital Evidence Characteristics

- Clearly Increasing
  - Evidence/Tool of the Crime
  - Storage is Cheap and Expanding
  - Sources expanding
- LEA Data Sources are Increasingly Digital
  - Sensors/IoTs
  - Mobile Wireless
  - Autos/Telematics
  - Audio/Voice
- Massive Growth of Police Video
  - Body Worn, In Car, Detention
  - CIP, Tactical, UAV, Crime Scene

Digital Evidence Challenges

- Largescale Distributed Network Storage/Complexity
- Rapid Technological Change/Complexity
- Issues addressing:
  - Data in Use vs.
  - Data in Motion vs.
  - Data at Rest
- Barriers to Access; Technical/Legal

Demographics - 2008 BJS CSLLEA

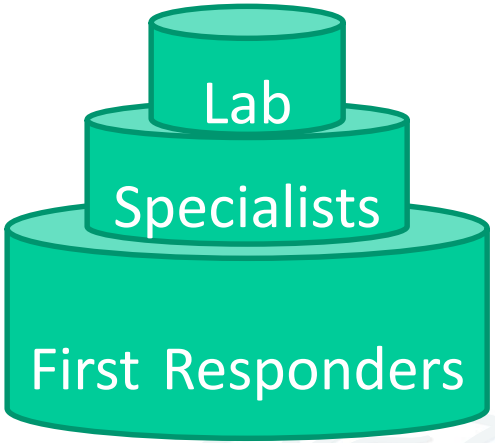
SLTT LEA 2008 Demographics

- 17,985 Agencies Total
- 13,096 Agencies < 25 Officers

= 73% < 25 Officers

SLTT LEA DE Handling

- Distributed Functions
- Lab vs. Field



2013 IACP Digital Evidence Research

- SLTT LEA Digital Forensic Partnerships:
  - Federal Task Force or Lab 25.5%
  - State Task Force or Lab 46.4%
  - Regional Task Force or Lab 36.4%
  - Local Partner or Mutual Aid 41.7%
  - Commercial Vendors 4.3%

  Total 154.3%

Universal Accreditation Policy Recommendation

- Mandates or Encourages DOJ/Non-DOJ FSSPs
  - Obtain and maintain accreditation
- What is an FSSP?

  "A person or entity that

  1) recognizes, collects, analyzes, or interprets physical or digital evidence AND

  2) issues test or examination results, provides laboratory reports, or offers interpretations, conclusions, or opinions through testimony with respect to the analysis of such evidence."
- Significant amount of SLTT LEA DE handling
  - Does normally Involve 1)
  - Does NOT always involve 2)
  - Potentially Analogous to Crime Scene Investigation and other field forensics

Universal Accreditation Policy Recommendation

- Additionally, the DOJ will
  - Require DOJ prosecutors to use accredited labs.
  - Use grant funding to encourage State and Local labs to pursue accreditation.

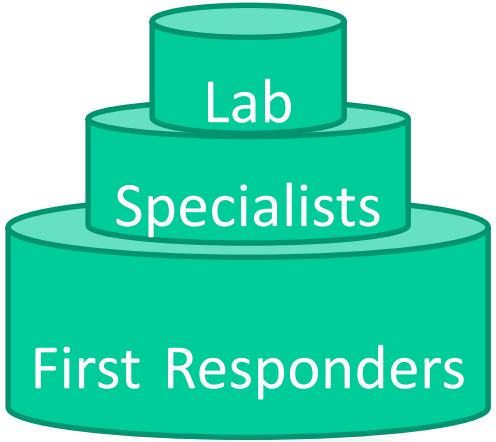
Appears to be a Federal Focused Policy?

Level of FSLTT LEA Integration?

Task Force Related Funding?

SLTT LEA DE Quality Management

- Tool Validation
- Certification/Proficiency Testing
- Quality Management/Peer Review



IACP/NW3C Polling

1. How does **tool validation** occur?
   - Local validation study with seeded evidence
   - Comparative tool limitation study with multiple tools
   - Manual validation of specific tool results
   - Mobile forensic tools – false negative variance
2. Is there any recurring process for **revalidation of tools**?
   - Validation or comparison frequency is based on change

IACP/NW3C Polling

3. How are **tool limitations** addressed?
   - Reporting and Documentation
   - Cataloging of Limitations
   - Alternate Tools
   - Tool revalidation
4. What is minimum **professional certification** for examiners?
   - No Single Standard…
   - IACIS CFCE
   - FLETC SCERS, NW3C, NCFI

IACP/NW3C Polling

5. What **quality control programs** are in place?
   - No Standard Program
   - Peer Review is most common
   - Standard Processes
   - Supervisory Review
6. What recurring **proficiency testing** occurs?
   - CFCE every 3 years
   - Some Certs/Tools every 2 years
   - Some Agencies every year

IACP Position

- Mandates and timing for accreditation must be tied to **adequate resourcing**; **appropriation of funds**.
- Application of universal accreditation to SLTT LEA or Non-DOJ FSSPs, should **remain voluntary**.
- Application of universal accreditation to SLTT LEA or Non-DOJ FSSPs, should **NOT affect eligibility** for **DOJ grant** money.
- Federal **Prosecutors should NOT be constrained** by accreditation of Non-DOJ FSSPs.
- **Definition of an FSSP** should **differentiate** between scientific laboratories and digital evidence investigation, digital evidence collection, digital evidence triage, and digital evidence examination.

Other Recommendations

- Creation of new ISOs precisely aligned with SLTT LEA DE handling and related field activities.
- Infusion of National resources into the tool validation process to speed up validation cycles and eliminate current gaps.
- Common DF certification and proficiency testing core curriculum.
- Development of state and regional models for cooperative peer review and quality management networks to address small agency needs.
- Development of model policy for SLTT LEA DE activities and handling.

IACP Law Enforcement Cyber Center

- For more information about the Center:
  - Email: cyber@theiacp.org
  - Website: www.IACPcybercenter.org
  - Access from the LEEP Portal