Defense Cyber Crime Center

A National Cyber Center

National Commission on Forensic Science

William Eber
Chief Technology Officer
DoD Cyber Crime Center

Overview

- What is the DoD Cyber Crime Center?
- Defense Computer Forensic Laboratory
  - DCFL Accreditation with ASCLD-LAB
- Continuing Factors for DCFL Accreditation
- Digital Evidence as a Forensic Discipline
- If Decision is made to Mandate Accreditation…
  - Tailored
  - Incremental

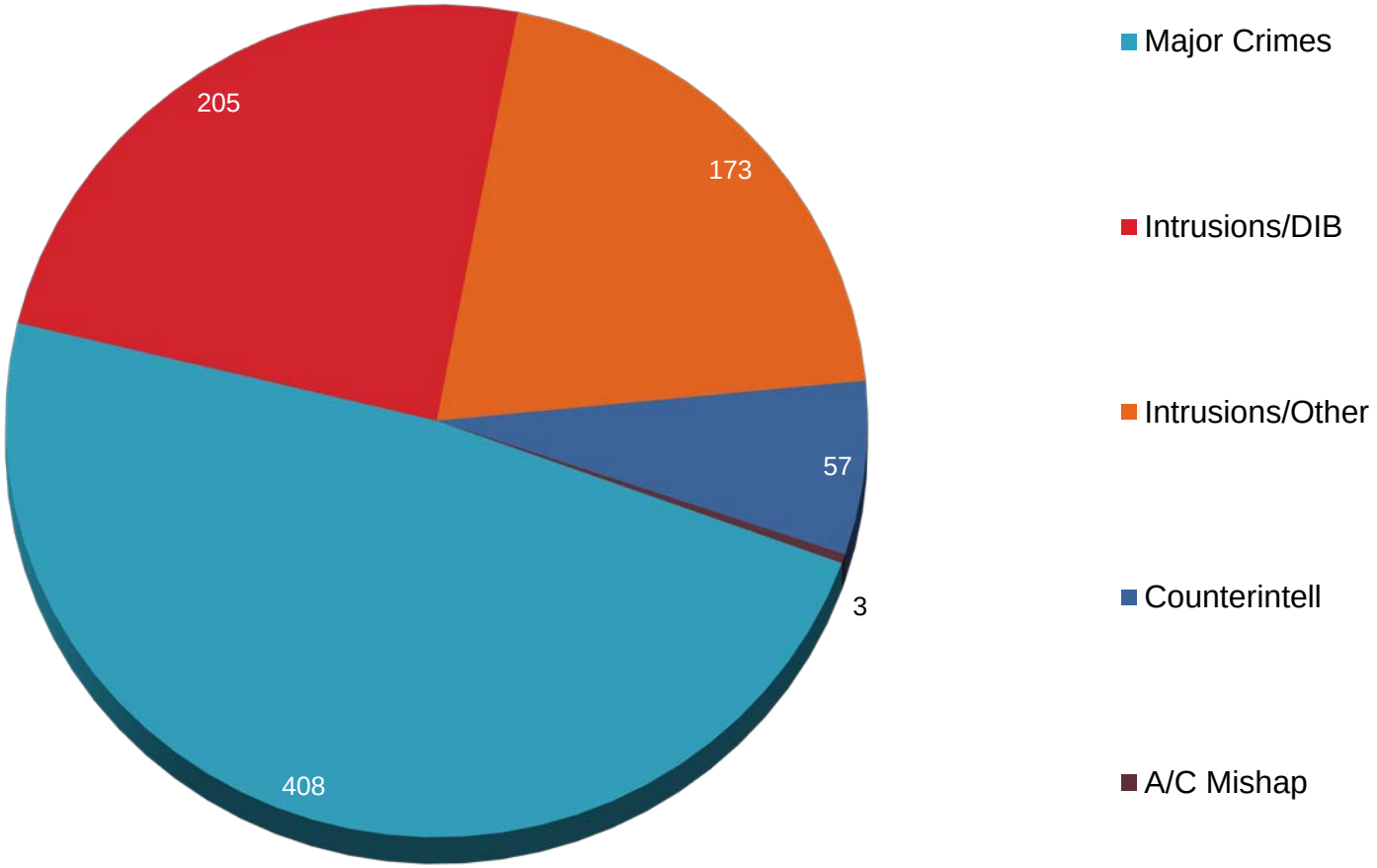
DC3 Operations

- One of 6 National Cyber Centers under NSPD 54
- A technical center for digital & multimedia (D/MM) forensics, cyber investigative training, technical solutions development, & cyber analytics supporting DoD requirements in:
  - Law Enforcement & Counterintelligence (LE/CI)
  - Information Assurance (IA)
  - Critical Infrastructure Protection (CIP)
  - Document & Media Exploitation (DOMEX)
  - Counterterrorism (CT)
- ~420 persons: 33% DAF civ / mil, DoD civ & USN pers; 66% contractors

A National Cyber Center

Forensics Lab

FY 16 YTD Forensic Exams – 846 / 507 TB



A National Cyber Center

Effective: 5 Nov 15

Laboratory Make-Up

- Evidence Intake (3 Employees) *
- Imaging and Extraction (13) / Advanced Data Acq (5)
- Major Crimes (24)
- Counterintelligence (14) / External Detail (6)
- Intrusions (19)
- Litigation Support (1)
- Quality Assurance (6) *
- Customer Support (3)

DCFL Accreditation with ASCLD/LAB

- Accredited under the Computer Forensics Testing Category / Digital & Multimedia Evidence Discipline
- One of the larger accredited computer forensics labs under one roof
- Initially accredited in 2005 under the Legacy Accreditation Program and migrated to ISO/IEC 17025 in 2011
- Recently hosted 6 Inspectors for the 5-year renewal
- 383 Potential Findings
- Yearly Reviews by 1 Inspector

Continuing Factors for DCFL Accreditation

- Quality Management System
  - Codify SOPs to take into consideration ISO/IEC 17025, ASCLD/LAB Supplemental, and local requirements
  - Maintain quality manual describing the quality system agile enough to allow for evolving technical challenges
  - Articulate achievable training requirements
    - What makes you proficient? Need testing program
    - Leading Edge capabilities, e.g., vehicle forensics
  - Set up peer review, admin review, and quality review practices

Continuing Factors for DCFL Accreditation

- Information Management System
  - Captures metrics – Tracks reviews
- Quality Assurance Manager
- Multiple networks – Classified and Unclassified data
  - Consistent processes across networks
- Configuration management Win/Mac/Linux & Legacy OS
  - Consistent software/hardware builds
  - Maintenance programs / Validation of Tools/Processes
  - Deviation process

Digital Evidence

- Relatively Nascent / Constantly Evolving
- Original evidence can be replicated and mathematically validated; no limit to number of copies
  - Original evidence will still be unchanged & secured
  - Copies may be distributed to various examiners, dependent upon lab processes
- Most important steps to increase accuracy / reliability
  - Peer review process / Comparative evaluation
  - Technical deviation tracking / Procedures and Tools
  - Regular solicitation of customer feedback

If Decision Made to Mandate Accreditation…

- ISO/IEC 17025 standard is high-level and does not dictate specific steps or checklists for a lab to perform work
  - Accrediting body generates supplemental requirements that are a bit more granular
- Consider differences in lab functionality
  - Forensic processes that capture data vs. Forensic processes that interpret data and generate reports
    - Potential for certification to ensure chain of custody
  - Spinning disks vs. mobile device vs. flash memory, etc.
    - Apply different supplementals

Proposed Tailored Accreditation

- **Influence / Draft (potentially through OSAC) Supplemental Specific to the Digital Evidence (DE) Discipline and Sub-Disciplines**
  - **Drives accrediting bodies to adopt supplemental requirements specific to sub-disciplines within DE**
  - **Opens the door for smaller labs to adhere to a subset of requirements that larger labs are held to**
  - **Core forensic competencies are non-negotiable**
  - **Allow for broader interpretation of management and other resource-intensive requirements laid out in ISO/IEC 17025**
- **Graduated process to allow for periodic re-evaluation to add or remove recommended processes; allows for capability growth**

Proposed Incremental Accreditation

- Develop 5-year Program Aimed at Assisting Labs toward Accreditation
  - Milestones / Accountability
  - Initially aimed at ensuring core forensic competencies
    - Quality management processes by default
  - Evolve toward management and oversight components
    - Influenced by capability-specific supplementals
  - Ability to rely on collaborative laboratory relationships without these laboratories necessarily being accredited to ISO/IEC 17025

Summary

- **Accreditation has its Pros and Cons, even for Larger Labs**
- **Digital Evidence Discipline is Evolving**
- **If Mandated, Developmental Factors should be taken into Consideration**

Questions?

A National Cyber Center

william.eber@dc3.mil
Office: 410-981-0103
Web: www.dc3.mil