

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

REVISED DRAFT

A Manager's Guide for a Computer Forensics Unit

National Center for Forensic Science

The National Institute of Justice

Revised April 2006

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

A Manager's Guide for a Computer Forensics Unit

- 1. Introduction**
- 2. Overview of Process**
- 3. Budget**
- 4. Staffing**
- 5. Training**
- 6. Retention**
- 7. Accreditation and Certification**
- 8. Management of a Computer Forensics Unit**

1. Introduction

“Digital evidence is information of probative value stored or transmitted in binary form” (SWGDE, July 1998).

Digital evidence has become a major source of evidence across all criminal violations and civil actions. Agencies have a strategic responsibility to deal with emerging crime trends and management must find ways of dealing with this rapidly increasing trend. What can you do?

Agencies that do not adopt policies and procedures, allocate resources, and define roles and responsibilities with respect to digital evidence are accepting the risk that their operations will fail to identify the guilty, repair torts, and protect the community. Given the demands of society in this increasingly technical age, this option is not likely acceptable. In all likelihood, agencies will need digital evidence capabilities in their most significant case at the most inopportune time. Only prior planning and effective management will prevent disaster.

This document is designed to assist law enforcement agencies, crime laboratories, and other organizations which are interested in the development, implementation, and management of a computer forensic program.

There are many options. Each organization needs to find the mission, structure, and resources appropriate to its situation. One solution is to develop an internal capability. A number of organizational structures will be discussed along with the advantages and disadvantages of each. Additionally, there may be an opportunity to outsource the agency's requirements to another agency, crime laboratory, regional computer forensic facility, or various commercial entities.

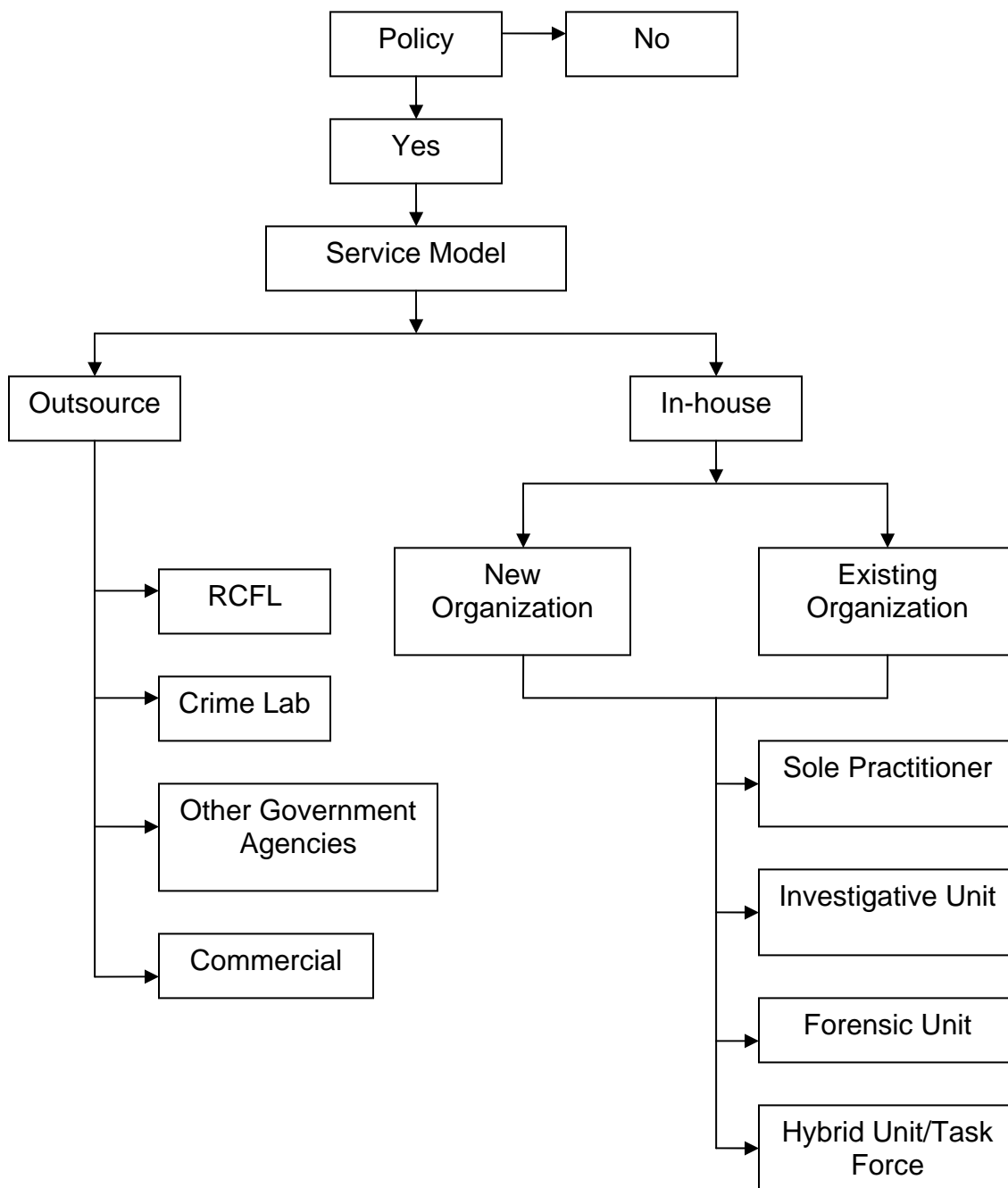
The following items need to be addressed when considering digital evidence:

- The establishment of a computer forensic program should be a strategic decision by senior management
- The program established should meet the current and future needs of the agency
- The examination of computers for evidentiary purposes is a salient component of current criminal activity
- There is nothing that currently indicates that this trend will do anything but expand
- As we have seen in the explosion of DNA forensics, the trend in digital evidence will likely grow exponentially. DNA is present in a portion of criminal cases, while digital evidence is becoming prevalent in virtually all violations.
- The criminal justice system, the legislative branch, and the public all expect that law enforcement agencies can protect the lives, property, and welfare of the community in both the physical and electronic worlds.

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

This guide is designed to assist executives and managers to understand both the nature of the problem and the range of solutions. The authors of this guide have collected their experiences from a wide range of law enforcement organizations. Nothing in this guide should be considered a requirement, but rather experience shared.

There are a number of things that must be done; this process has been mapped below:



DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

- Establish policy
- Define organizational structure (i.e., service model)
 - ▶ Conduct examinations in-house
 - New organization
 - Existing organization
 - ▶ Outsource examinations
 - Regional computer forensic laboratory (RCFL)
 - Crime laboratories
 - Other governmental agencies
 - Commercial organizations

Note:

- Both law enforcement and commercial outsourcing are difficult to budget; there is usually no control over prioritization of case work
- Outsourcing is expensive

If you are going to provide service internally, a number of issues have to be addressed:

- The very first question that management must address concerning doing digital evidence within the organization is: “Is it an investigative function or a crime laboratory function?” Actually, it is both, but you must define responsibilities and allocate resources accordingly.
- Computer forensic services can be provided either within a law enforcement agency or by a dedicated forensic laboratory. Within a law enforcement agency, there are a number of organizational structures, which include:
 - ▶ Sole practitioner
 - ▶ Investigative unit
 - ▶ Forensic unit
 - ▶ Hybrid Unit/Task Force

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

Each of these organizational structures will be discussed further in this document. Within a forensic laboratory, the services can be provided in a computer forensic unit; an audio/video unit; or a digital evidence unit.

Each of these organizational structures has advantages and disadvantages. Several of these service models may be combined. Some of these models integrate well with existing organizational structures. However, some organizational structures make it difficult to maintain a quality product.

2. Organizational Structures

▪ SOLE PRACTITIONER

- ▶ A single individual, usually sworn, assigned to a law enforcement unit whose primary responsibilities are other than the provision of forensic services.
- ▶ The individual is assigned both forensic and investigative duties
- ▶ The individual may perform both functions on the same case
- ▶ This model may be the only practical solution for smaller agencies
 - Advantages
 - Quick to implement
 - The initial cost of entry is relatively inexpensive (although long-term costs are equivalent to other solutions)
 - The duty assignment is very flexible
 - Tight integration with the organization's mission
 - Disadvantages
 - Limited qualifications/capability (a single individual cannot maintain a complete set of skills)
 - Difficult to maintain skills (because duty assignment is flexible)
 - Little quality control (e.g., peer and administrative review of casework)
 - Time management issues
 - No redundancy
 - Administrative/logistic overhead costs
 - High burn-out rate ("burning the candle at both ends")
 - Productivity statistics are problematic and difficult to compare with other unit personnel
 - Impossible to scale
 - Management Issues
 - Manager has little knowledge of subject matter
 - There is usually little oversight
 - The manager often does not "see the train wreck until it happens"

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

- Productivity statistics are difficult to compare with other unit personnel
 - The sole practitioner becomes the “digital god” in the department
 - There are few career/promotion opportunities if the individual is dedicated to technology
- Other issues
 - No separation of investigative and forensic function.
 - Investigator has to be both fact and expert witness
 - Potential conflict of interest
 - All of the “eggs are in the same basket”
- **INVESTIGATIVE UNIT**
 - ▶ An investigative unit, for the purposes of this document, is defined as a unit comprised of sworn personnel whose primary responsibility is conducting investigations of high tech crimes and forensic examinations in connection with those duties. The unit may also provide digital forensic services to other units
 - ▶ Personnel may often perform both forensic and investigative functions on the same case
 - ▶ These units are typically contained within the investigation division
 - ▶ Management is within the investigative branch and is driven by investigative metrics
 - Advantages
 - The investigative unit puts all the resources together, which creates synergy
 - Multiple investigators can compensate for individual weaknesses
 - Economy of scale due to the ability to share resources
 - Potential ability to conduct peer and administrative review of casework
 - increased supervision
 - provides some redundancy
 - allows for apprenticeship and a career path

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

- Disadvantages
 - Relatively expensive to create and sustain
 - large continuing budget/personnel commitment
 - lack of dedicated forensic space and equipment
 - need to constantly increase in size due to the increasing amount of digital evidence seized across all violations
 - difficult to scale (i.e., organizational, management, personnel issues, and policy issues resulting from multiple units)
- Management Issues
 - Supervisor must be competent in all three disciplines (investigative, forensic, and management)
 - competing needs for investigation and forensics for other units (i.e., management reports to its own “chain of command”)
 - investigative program which houses the unit drives the services provided
 - there is no owner of forensic overhead (i.e., investigative programs do not want to support non-investigative overhead, such as proficiency testing, quality assurance, and forensic training)
 - the level of quality is defined by policy and management
- Other Issues
 - Investigative, forensic and analytical processes are all served by the same individual and management
 - Creates a lack of separation which may cause concern from a litigation standpoint
- **FORENSIC UNIT**
 - ▶ A forensic unit, for the purposes of this guide, is an entity whose mission is to provide computer forensic services for investigations
 - ▶ This unit is staffed by sworn and/or non-sworn examiners and technicians meeting laboratory accreditation standards
 - ▶ Forensic personnel do not serve an investigative function, although they may provide technical support
 - ▶ Dedicated space and resources are required

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

- ▶ Unit may be placed in a variety of locations within the organizational structure
- ▶ Management metrics are forensic rather than investigative
- ▶ Many managers have forensic experience
 - Advantages
 - Dedicated space is designed for a single purpose
 - Standard Operating Procedures (SOPs) and quality assurance guidelines that are specific to computer forensic examinations
 - A defined business process, the focus is digital evidence examination, fixed business process yields quality, and it is very scalable
 - Dedicated personnel (e.g., examiner, technician, property custodian, support staff) and clear division of labor/responsibility
 - Efficient use of space, people, training, and equipment
 - Disadvantages
 - Expensive to establish and maintain
 - requires dedicated space
 - full overhead costs (time and personnel) of quality assurance
 - Requires additional personnel, training, equipment and line-item budget
 - Limited career path opportunities
 - Management Issues
 - Requires dedicated personnel documentation (job descriptions, performance appraisals, etc.)
 - A technically-competent manager
 - A quality management system
 - A line-item budget
 - A performance measurement system
 - Need for cadre of examiners or long ramp-up time, discipline changes and grows faster than other disciplines necessitating higher levels of recurrent training and education

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

- Other issues
 - Full separation of roles
 - Potential for less direction from outside sources (i.e., prosecution, defense, investigators, etc.)

- **HYBRID UNIT/TASK FORCE**
 - ▶ A hybrid unit/task force, for the purpose of this document, is defined as a unit whose stated mission is to provide both investigative and forensic services

 - ▶ Personnel are separated by function (e.g., some serve as investigators, and others as examiners) but managed as a single unit

 - ▶ The unit usually operates under the administrative control of the investigations branch, and sometimes as a task force

 - ▶ The unit sometimes serves a region
 - Advantages
 - All the advantages of both investigative and forensic units, added synergy (e.g., investigators and examiners appreciate each other's capabilities)
 - Scalable

 - Disadvantages
 - Complex to manage
 - competing (both internal and external) interests
 - pressure to break-down division of labor
 - tendency to exceed individual training and expertise

 - Management Issues
 - Most difficult to manage
 - management of success is entirely internal
 - expectations are entirely external - too many masters

 - Other issues
 - Contamination issues if space is not separated
 - all functions under same "roof"

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

- Difficult to determine exactly what was done in a particular case - accountability for actions

3. Budget

Computer forensics is very different from traditional law enforcement operations. In many ways, it is similar to starting and operating a business. It requires a large amount of initial capital, personnel costs, training costs, recurring consumables to produce a forensic product, and is expensive to maintain. As a result, the development of an appropriate budget specifically for computer forensics is critical. Failure to budget adequately a forensic program will result, eventually, in a failure of the program. When creating a budget, consider the following:

- Funding issues
 - ▶ Is the funding a line item?
 - ▶ Is the funding in the form of a “fee for service”?
 - ▶ Is the funding source a grant of some type?
 - ▶ Is the funding continuous, or is it one-time?

- Initial startup costs
 - ▶ Initial facility construction/renovation costs
 - ▶ Personnel costs
 - ▶ Initial training costs
 - ▶ Initial support services costs (administration, quality assurance, evidence control)
 - ▶ Initial equipment (hardware and software)

- Recurring costs
 - ▶ Recurrent training
 - ▶ Consumables (most computer forensic cases have direct media costs, such as: hard drives, optical disks, paper)
 - ▶ Equipment upgrade and maintenance
 - ▶ Facility costs (utilities, maintenance, communications)
 - ▶ Operational support costs (administration, quality assurance, evidence control)

Note: Recurring costs are typically fifty-percent of the start-up costs per year

- Equipment purchase considerations
 - ▶ Do not categorize computer forensics equipment under “IT” for procurement purposes

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

- ▶ Home/office PCs are usually idle and full capabilities are rarely tapped. Most forensic computers utilize their full capacity. Therefore, always purchase the highest-end equipment that the budget will allow
 - It is about function, productivity, and services provided
 - The amount of data to process doubles every 18 months (which necessitates doubling the technology capability every 18 months)

- ▶ Do not underestimate the costs for designing, building, and furnishing a unit. Such costs include:
 - Furniture
 - Utilities
 - Redundant power
 - Power conditioning
 - Internet connectivity
 - Telecommunications (including cell phones)
 - HVAC (Heating, Ventilation, and Air Conditioning)
 - Cabling
 - Security
 - Evidence and supply storage

- Personnel costs
 - ▶ Where do you secure the staffing to conduct computer forensic examinations?
 - Two choices:
 - Use existing position(s)
 - Create new position(s)

 - ▶ What type of position are you trying to fill?
 - Investigator?
 - Examiner?
 - Analyst?
 - Support?
 - Administrative and Q/A
 - Evidence control

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

- Custodial
- Network administrator

- ▶ Is a “Sworn” person more expensive than a “non-sworn”?
 - “Sworn” is generally more expensive when factoring in overtime and retirement (to a point)
 - The overhead for sworn is greater than for non-sworn (training can take up to 25% of Full Time Equivalent or FTE)

- ▶ How do you pay overtime?
 - The way in which overtime is paid varies (Fair Labor Standards Act [FLSA] Exempt versus non-exempt)
 - What about an agency’s ability to afford/control overtime?

- ▶ What personnel issues might be involved?
 - Union contracts
 - MOAs/MOUs (for task forces and RCFLs)

- Vehicles are an important tool for examiners and must be included in the budget
 - ▶ Do you rely on a “pool” of vehicles for both sworn and non-sworn?
 - ▶ Do you need specialized vehicles? Will a field response kit suffice?

- Outsourcing of computer forensic casework
 - ▶ You may need to outsource the following:
 - Evidence items that you do not have the capability to exam
 - Data recovery services for damaged media
 - Backlog reduction
 - Conflict of interest cases

4. Staffing

The quality of the forensic program in large measure is a result of the people assigned to the program. Selection of the best candidate(s), proper training, career development, and retention are key issues to ensuring the success of the program.

- Are the selection criteria in place?
 - Regardless of the size of the program, an objective selection criteria should be utilized
- What are management's expectations? How long does the organization expect the person to be in the position?
- Are the selection criteria consistent with the position description?
- What are the prerequisites for education, experience, and certification?
 - Will you bring someone in with the experience needed?
 - Will you train someone from within your organization?
 - How do we identify candidates who are properly motivated and who have characteristics which will allow them to become a successful examiner?
- Is the position "sworn" or "non-sworn"?
- Have you addressed the "chain of command"?
 - Where do you place someone?
 - What are their responsibilities?
 - Where do you place the computer forensic unit?
 - The organizational structure tends to drive the mission.
 - For the sole practitioner, who they report to determines the success of the digital forensic program
- Do you have position descriptions?
 - Forensic
 - Investigative
 - Support

Reminder – reference CART and DEA position descriptions in an appendix

- What is your recruiting strategy?

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

- ▶ Advertising
 - Newspapers/journals
 - Forensic associations (AAFS, MAAFS, ASCLD, CAC)
 - College and university forensic/computer science programs
- ▶ Geographical work location
- ▶ Screening/evaluation
 - Review resume and training
 - Oral/written examination
 - General IT questions
 - Forensic questions
 - Selection panel
 - Background/medical clearance
 - Salary and benefits (see “Retention”)
 - Professional development
 - Hours/work schedule
 - Training (see “Retention”)
 - Career Pathing (see “Retention”)
- Hiring and managing
 - ▶ Testing (competency and proficiency)
 - ▶ KSA's (knowledge, skills, and abilities)
 - ▶ Performance appraisals

5. Training

The practice of computer forensics requires an extensive set of knowledge, skills, and abilities. Computer forensics involves examination of a wide range of hardware and software. There is a tendency for examiners to specialize in particular hardware, software, and/or examinations. In addition to these KSAs, practitioners must be able to document formal training and demonstrate competency in their assigned specialty. Management must ensure that examiners demonstrate not only the KSAs but the education and training which supports them. Continuing education requirements may be imposed by agencies, accrediting bodies, certifying bodies, and professional organizations (e.g., ASCLD-LAB requires 40 hours of training per year per examiner). Some agencies may choose to require other specific training requirements. Due to the rapid evolution in digital forensics, neglecting ongoing training and professional development will result in decreased capability and may lead to program failure. Agencies should develop a training plan based on current practices and technology.

It is important that computer forensic examiners understand both the discipline of forensic science as well as the criminal justice system. In order to ensure this, training should be designed to ensure that sworn examiners are thoroughly versed in forensic science methodologies. Non-sworn examiners must be trained not only in forensic science methodologies but must receive formal training and experience in the criminal justice system. It is important that examiners embrace the corporate culture of criminal justice.

- Types of training
 - ▶ Initial training
 - Define training requirements
 - Services provided will determine the level and amount of training; services should only be provided for which adequate training and prof/comp testing have been successfully completed
 - ▶ Core training
 - Basic computer science
 - Basic hardware and software technology
 - Basic networks
 - Basic computer forensics
 - Basic computer search and seizure
 - Tool-specific forensic training
 - Operational (“on the job”) training
 - Evidence handling and quality assurance
 - Legal/courtroom training

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

- ▶ Recurrent training
 - Technical, operational, and tools-specific training as required on an ongoing basis
 - Attend relevant conferences, workshops, exhibitions, and symposia
- It is important to understand the difference between education and training
 - ▶ Education from accredited colleges and universities is recommended to ensure long-term performance of forensic personnel
 - ▶ Training is designed to provide specific knowledge, skills, and abilities directly associated with the job.
 - Forensic examiners need both education and training to maintain currency.
- Customer/external user training
 - ▶ Not only do the members of the computer forensic unit need training, but providing training to the user base has proven both effective and efficient in managing digital evidence workflow.
 - ▶ Time should be allocated for examiners to provide training to customers, including attorneys, law enforcement, and judges.
 - ▶ This training should focus on the services available from the unit, the sources of digital evidence, the seizure, and preservation of digital evidence.
- Staffing for Training (see “Staffing”)
 - Providing forensic services is more than conducting search and seizures; you also need training, the time to learn new tools/technology, and time to teach customers (all of which require staffing and resources). At some level of activity, it will be necessary to devote dedicated personnel to the training function. Training costs money, and someone has to do the paperwork to pay for it
 - Agencies must have sufficient staffing in order to provide an acceptable level of service while examiners are undergoing training.
- Agencies should consider training partnerships with the following:
 - ▶ Colleges/universities

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

- ▶ Task forces
- ▶ RCFLs
- ▶ Non-profit training organizations
- ▶ Local, State, and Federal agencies
- ▶ Professional societies and organizations
- ▶ Private industry

Building a dedicated computer training facility in connection with a comp forensic unit has proven to be very efficient and effective.

6. Retention

It is difficult and expensive to recruit, train, certify, and manage computer forensic examiners. Retention of these valuable resources is crucial to the long-term success of a computer forensic program. There are many elements involved in retaining good examiners, whether they are sworn or non-sworn.

Sworn examiners often enter a computer forensic program early in their career, and remain there until they leave for promotion. Organizations should consider career paths which will allow expensively trained examiners to remain within the field. It takes a number of years for an examiner to gain the training and experience necessary to be efficient. Consideration should be given to ensuring that an employee will have sufficient years of service remaining in order to be fully utilized.

Non-sworn examiners face a different situation. They often have better job prospects because they usually have more technical education and background than that of sworn examiners; this might make them more attractive to the private sector. Non-sworn examiners working for government agencies are therefore more likely to leave for higher-paid positions in the private sector. Non-sworn examiners may leave their positions in government because there is a perception of work that is more interesting, better facilities, and resources in the private sector. While this might not always be the case, the perception persists.

The primary motivator for successful examiners is a sense of public service. Examiners enjoy at a very basic level being involved in law enforcement and forensic operations. The pay, the benefits, and the working conditions must be sufficient to meet the needs of examiners. When they are not sufficient to support the examiners' personal needs, then they will seek opportunities either in another agency or in the private sector. Managers should not underestimate the dedication to public service by technical employees.

The following bullet points will provide some suggestions.

- Recognition
 - Recognition of individual employees for their dedication, work, and success is especially important in the public sector. However, examiners need and want to feel like they are appreciated as members of the criminal justice team. Formal acknowledge of their activities can be a very effective motivation and retention tool which is inexpensive and can be carried out in the following ways:
 - Public (e.g., press releases, media interviews, public speaking, teaching)

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

- Peer (e.g., certificates, plaques, employee of the month, case assignments)
- Case recognition (i.e., timely recognition for overcoming difficult working conditions and technical challenges)

- Incentives
 - Personnel
 - Pay for performance
 - Professional development (continuing education and training)
 - Tuition reimbursement
 - Longevity recognition
 - Pay
 - Leave
 - Sabbatical

 - Career Path
 - Professional associations (paid for by agency)
 - Take-home/response vehicle

 - Working condition
 - Types of preferred assignments
 - Job flexibility
 - Flexible hours/shifts
 - Telecommuting
 - Administrative “time off”

 - Travel
 - Casework
 - Conferences/workshops

 - Access to state of the art equipment
 - Laptops
 - PDAs
 - Cell phones

7. Accreditation and Certification

It is important to understand the difference between accreditation and certification. Accreditation is the formal recognition by an accreditation body that an organization has policies and procedures considered appropriate to their mission and operates according to those policies. Accreditation is about the organization. In the law enforcement community, the most common accreditation is the Commission on Accreditation of Law Enforcement Agencies (CALEA). The equivalent accreditation for forensic organizations is the American Society of Crime Lab Directors-Lab Accreditation Board (ASCLD-LAB) and ISO 17025. It should be noted that several states have passed legislation mandating organizations performing forensic examinations to be accredited under ASCLD-LAB or ISO 17025.

Certification is the recognition that an individual possesses the knowledge, skills, and abilities (KSAs) to perform professionally their duties. Traditionally, forensic laboratories have certified their employees internally. Over the last several years, a number of forensic disciplines have developed certification programs through organizations such as the American Board of Criminalistics (ABC). The International Association of Computer Investigative Specialists (IACIS) has offered certification for graduates of their program in computer forensics. There is currently in development a forensic community certification body for digital forensics, which includes computer forensics, and is called the Digital Forensics Certification Board (DFCB).

There are certifications based upon commercial products and the completion of training related to them, as well as general professional certifications. These certifications are valuable indicators that an examiner has received specific training, and is recommended that these be obtained in addition to forensic certification. Consideration should be given to obtaining widely accepted certifications. Both have value in regards to demonstrating the technical competence of examiners.

It must be recognized that any agency that allows an employee to conduct computer forensic examinations is in effect certifying the competency of that individual, and is accepting liability for their actions.

8. Management of a Computer Forensics Unit

It is important for all managers to “own” the mission of their organization. But this is especially important for managers that do not have personal experience in the field. It is not uncommon for non-technical (both sworn and non-sworn) managers to supervise computer forensic units. Ownership includes a thorough understanding of the business process and tools used to accomplish the unit’s mission. This does not require that managers become technically proficient but it does require a thorough understanding of the principles and practice. Managers without a technical background need to expend the effort to understand both the technology and the process of digital forensics.

Managers need to abide by the principles of “lead up” and “support down”. One of the critical functions for managers of tech programs is to act as effective advocates to executive management in the areas of personnel, budget, and policy. In order to perform these duties effectively, managers must be able to educate their peers and leaders on the technical issues. One effective technique is to have available an “elevator speech”, this is a very short (i.e., 30 seconds) presentation covering the following topics:

- What do you want?
- What do you need?
- How are you going to present it?
- How are you going to benefit the organization?

Conversely, managers must identify and support the needs of their subordinates. Managers must develop a working relationship with their subordinates wherein each recognizes and appreciates their respective roles and responsibilities.

One of the critical means of ensuring that both management and employees are working together is to develop and effectively communicate a vision for the organization. Employees will understand the direction that the unit is going and will be able to support that evolution.

Technology is “visionary” (some would describe it as “bleeding edge”). Managers must act as visionaries within their organizations because computer forensics will likely be one of the most technically advanced aspects of a criminal justice agency. Units and organizations which do not actively adopt new technology and techniques will in short order become ineffective

The environment in which computer forensics operates is dynamic both with respect to the technology and the criminality. Both of these dimensions are changing at a pace far more rapidly than traditional crime. As a result, managers of computer forensic programs must manage more strategically. They must anticipate how

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

change will affect their staffing, training, and budgets. The managers should look two to five years ahead, and develop formal plans for a two to five year horizon.

There is an old management adage that you should measure what you manage and manage what you measure. Both employees and managers need to understand what is important to an organization. In both law enforcement and forensic science, one of the traditional measures is statistics or “stats”. Selecting and implementing statistics for a digital forensic unit is crucial to ensuring that they are operating in a way that benefits the organization. If currently available, statistic measures do not reflect the actual work of members of the unit or if they conflict with the desired work of examiners, then management must develop statistics which will more adequately reflect both the mission and the practice.

Statistics can also be an effective way to manage the way in which individual examiners approach their duties. As an example, if we only count the number of cases assigned to an examiner, then there is not a statistical motivation to complete cases. Conversely, if we only count reports written, then we are encouraging minimal examinations. We measure effort, but effort doesn't necessarily translate into “productivity”. It is suggested that the two measures can be balanced by defining examination goals for each examination and measuring completion of those goals.

A third area in which statistics are very important is in the staffing and budget arena. Well designed statistics can support budgetary requests and demonstrate the positive impact that the comp forensic unit has on the organizational goals.

Managing Technical People

It is important for managers to understand the three environments in which computer forensic examiners work: 1) they operate in the role of an examiner; 2) they often serve as analysts; and 3) in some cases operate as investigators. Each of these roles has a different set of KSAs as well as different methodologies. As examiners, they are bound to be meticulous and adhere to scientific principles. As analysts, they are expected to synthesize both the results of the examination and the crime. As investigators, they are expected to manage the process and bring all available resources to bear on the case. It should be obvious that there are a number of conflicting requirements within these three roles. Management must take care to ensure that employees operate within their appropriate roles and remain within their scope of their expertise.

Managers need to be careful to manage “role creep”. This is the tendency for employees to be asked to perform duties beyond their assigned responsibilities. For an example, an investigator might request an examiner to review the case investigation and analyze the computer media to develop leads. While examiners

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

may have this capability, it will be extremely difficult to manage their forensic caseload, as it will be, in large measure, driven by the pace of investigations. Further, the examiner is not utilizing their specialized knowledge but rather general investigation skills.

Supervisors should manage employees within their specific roles utilizing metrics appropriate to the goals and objectives for that role. It would be inappropriate to evaluate an examiner based on convictions. That is clearly a metric appropriate for investigators.

Computer forensic examiners always bring a mix of skills and experience to the job. Managing these individuals to a level of excellence requires leaders to understand the skill set, interests, and personality traits of each individual examiner and utilize these to motivate each individual. By utilizing each examiner to their fullest capability, the unit will be most productive. Additionally, managers should carefully encourage examiners to develop a broad range of skills.

Examiners are very proud of their mastery of the technology and wish to be appreciated for that knowledge. Managers will greatly improve their relationship with examiners if they take the time to understand and appreciate the technical skills of their employees.

“Manage the Process”

Because of the large and increasing number of cases, the perpetual lack of resources, and the rapidly changing environment, it is very easy for units to develop unacceptable back logs. While additional personnel and resources can be effectively used to reduce the back log, managers should seek to control the business process. By managing workflow, supervisors can mitigate a great deal of stress on examiners and eliminate non-productive activities.

Appendix 1. Resources and Links

American Academy of Forensic Sciences (www.aafs.org)

American Society of Crime Laboratory Directors/Laboratory Accreditation Board (<http://asclid-lab.org/>)

Federal Bureau of Investigation (<http://www.fbi.gov/>)

High Tech Crime Task Forces (<http://www.hightechcrimecops.org/links.htm>)

High Technology Crime Investigation Association (HTCIA) (<http://htcia.org/>)

The International Organization on Computer Evidence (<http://www.ioce.org/>)

The International Association of Computer Investigative Specialists (<http://www.cops.org/>)

Los Alamos Laboratory (<http://www.lanl.gov/worldview/>)

National Center for Forensic Science (<http://www.ncfs.org>)

National Institute of Standards and Technology, Office of Law Enforcement Standards (<http://www.eeel.nist.gov/oles/>)

National Law Enforcement and Corrections Technology Center (NLECTC) Regional Centers (<http://www.oletc.org/regional.asp>)

National White Collar Crime Center (www.nw3c.org).

Regional Computer Forensic Laboratories (<http://www.rcfl.gov/>)

Scientific Working Group on Digital Evidence (<http://www.swgde.org/>)

U.S. Department of Defense Computer Forensic Laboratory (<http://www.dcfll.gov/>)

U. S. Drug Enforcement Administration, *Microgram Bulletins*, "Computer Corner" (<http://www.dea.gov/programs/forensicsci/microgram/index.html>)