Armstrong Police Cyber Forensics Division
Recommendation for the State Transformation in Action Recognition (STAR) program.

1. How long has the program operated? What was the month and year of initiation?

The Armstrong State University Police Department opened the Cyber Forensic Division's lab doors to the Criminal Justice community on January 1st of 2013. The lab has run digital forensics on devices at no cost to the state on a 24 hour 7 day a week basis since that time.

2. Has the program been in operation for nine months to three years? (Note: to qualify, the program must be between nine months and three years old as of May 29, 2015.)

Yes

3. Why was it created? What problems or issues was the program designed to address?

The use of digital devices by criminals has exploded in recent years. The District Attorney for Manhattan, Cyrus Vance, may have said it best when he stated: "Cybercrime is the fastest growing crime trend in New York and around the country". Yet, throughout the country, digital forensics labs are mired in backlogged cases. Federal, state, and local labs are reporting an exponential increase in the volume of digital devices submitted for examination that greatly exceed the capacity of the labs. Many states, such as Georgia and Alabama, report that the digital forensics labs have a seven to 19 month backlog of digital devices awaiting examination. In many cases, investigators are not submitting digital devices for analysis because they cannot place the case on hold for this long. Courts and prosecutors are increasingly concerned about these delays and the effect upon the due process rights of the defendant.

4. What are the specific activities and operations of the program? (Please list in chronological order, if applicable.)

Additional capacity is needed, but budgetary restrictions and limited resources make it unlikely, if not impossible, that help is on the way. The funds are simply not available to dramatically increase digital forensics capability for our criminal justice agencies, so some agencies are training a single employee to use a single piece of equipment. The problem is that no single piece of equipment can successfully access all types of digital media and a single employee cannot keep up with the technological advances and case load in digital media.

Chief Willcox created a Cyber Forensic Department in the University Police to address a growing problem throughout the State of Georgia and the United States. He also knew that anything he created would need to be relevant and support the academic function of the University. Making the department relevant meant that the department had to directly connect and show value to all areas of the University, including the academic and community outreach functions. His plan was that all patrol officers would receive training and certification in digital forensics analysis and investigations and a portion of the officers' uncommitted time would be spent examining digital devices for the criminal justice community and in providing the University's criminal

justice students with practical digital forensics internships. The students would be offered an approved 14 week internship in digital forensics where they would learn how to use state of the art digital forensics hardware and software. They would never work on evidence, but would work on devices and cases that replicated a real life environment. At the end of the 14 week internship, the students could choose to take a national certification examination in digital forensics from Access Data.

5. What equipment, technology and/or software (if any) are used to operate and administer the program?

In 2012, the department started training 5 police officers in digital forensics by partnering with NW3C, Mississippi State's Digital Forensics Department, and AccessData. The training was held in the Armstrong Police Department and the training was free. In January 2013, the Armstrong State University Police Cyber Forensics Division (CFD) opened their doors for business with trained analyst/investigators and a state of the art lab. The investigations include homicides, robberies, sex crimes, financial crimes, identify theft, burglaries, car thefts, prostitution and many other felony and misdemeanor crimes.

The University System of Georgia ended the Basic Law Enforcement Training Program in 2013. In exchange for managing the closing of the program, the University System of Georgia provided the Armstrong Police Department with funds that the department used to purchase the initial digital forensic equipment. This included three Forensic Evidence Recovery Devices (FRED) a Cellebrite machine, and licenses to use AccessData, Encase, and Lantern digital forensics software.

6. What are the annual operational costs of the program? How is it funded?

By placing the division within a university police department which has significant uncommitted time, hiring additional officers to perform CFD tasks is unnecessary. This model is built on the premise that once assigned a case, it is up to the officer to manage his or her time along with their other duties with the understanding that the lab needs to have an officer or technician available 24 hours a day for incoming and urgent requirements.

Funding for the renewal of software licensing is provided by the Armstrong Police Department's existing budget. The department does not receive additional funding for the Cyber Forensic Division.

7. Has the program been effective at addressing the problem or issue? Please provide tangible results and examples.

The Armstrong Cyber Forensic Division has reduced the backlog of digital forensics cases from seven to twelve months to less than thirty days for almost half of the State of Georgia for

federal, state, and local criminal justice agencies. The Armstrong approach has been so successful that other digital forensics labs are sending devices to Armstrong when they have been unable to access the device. Armstrong is successful where others have failed because we have acquired multiple hardware and software platforms and the analysts/investigators are encouraged to use all of the resources in analyzing devices. In a traditional lab, technicians often are working alone. We have found the old axiom two heads are better than one is not just a cliché. Officers and technicians are able to bounce ideas and experiences in discussions which creates a shared knowledge base when working with the ever evolving new technology as each previous model is updated and revised to entice consumers to buy the latest new gadget.

- Evidence developed for felony crimes, include homicides, sex crimes, robberies, burglaries, financial crimes, and criminal conspiracies
- The commander of the CFD is an attorney and cyber-crime expert, and is the source for Legal advice on digital crime law for police officers and district attorneys
- Agencies using CFD services at no charge include:
    - FBI
    - ATF
    - DEA
    - Secret Service
    - Georgia Bureau of Investigation
    - Georgia State Patrol
    - Georgia Department of Revenue
    - Georgia Probation
    - Chatham District Attorney
    - Chatham Narcotic Task Force
    - Savannah Chatham Metro Police
    - Dozens of area law enforcement agencies

The significance of timely digital forensics capability becomes apparent when digital evidence is uncovered for traditional crimes, such as burglaries, robberies, and thefts. These cases were brought to the CFD:

- Robbery case evidence included deleted text messages from a suspect's phone concerning the planning of the robbery and confirming that the robbery was committed.
- Theft case evidence included deleted photos from a suspect's phone, showing pictures of the stolen items and references to the lawful owner.
- Probation violation evidence included deleted photos from a suspect's phone, showing the suspect holding a gun, whose serial number is visible in the photo. Follow up investigation determines the gun to be stolen.
- Sexual assault case evidence included deleted photos from a suspect's phone showing the victim handcuffed and nude on the date and time of the crime.

- Auto theft case evidence included deleted videos from a suspect's phone showing the suspect and others in several other stolen cars with guns and drugs.
- Narcotic investigation recovers deleted photos of government officials with narcotics traffickers from a Blackberry device.
- Narcotics investigations recover real-time intelligence information from seized phones and computers.
- A robbery suspect is identified through a single video frame of a deleted video from a seized phone.
- Theft suspect's phone reveals that suspect was selling stolen items through Craig's List.
- Evidence was obtained from a computer professional's computer print spool after the suspect wiped files from computer.
- In a child molestation case data was retrieved from the suspect's computer that lead to the discovery of dozens of additional victims.

8. What measurable impact has the program had? Has it created significant change in your state?

The significance of this submission is that Chief Willcox took a small, 18 officer, campus police department in southern Georgia was able to redefine its role in the greater criminal justice community to arrive at a solution for this criminal investigative problem that has eluded federal and state government. In the process, hundreds of felony criminal cases for dozens of criminal justice agencies have been positively impacted. Since January 1, 2013, more than 1000 devices for over 400 federal and state criminal cases have been processed in 30 days or less, these cases would have otherwise sat untouched in an evidence room for 7 to 19 months. The evidence that was discovered included videos of crimes, pictures of stolen property, text and email messages about participation in criminal activity, and other evidentiary documentation of criminal activity and involvement for agencies such as the FBI, ATF, DEA, Secret Service, Georgia Bureau of Investigation, Georgia Department of Revenue, Georgia State Patrol, Savannah-Chatham Metro Police, Multi-agency drug task forces, and many other agencies.

The impact of this initiative is that the backlog for the southern half of the State of Georgia is 30 days or less, while the northern half of the state still has a 7 to 12 month backlog of cases waiting processing. The Armstrong lab has become the largest state of the art digital forensics lab in the state in less than two years. The Armstrong State University Department's program is innovative and has positive implications for criminal case investigations on an unprecedented level. I believe that no other campus police department has had such an immediate and long term impact on so many criminal investigations for so many agencies.

9. Did the program originate in your state? If YES, please indicate the innovator's name, present address, telephone number and email address.

Armstrong Police Cyber Forensics Division
Recommendation for the State Transformation in Action Recognition (STAR) program.

The Cyber Forensic Division is the brain child of the Armstrong State University's Chief of Police Wayne Willcox.
Armstrong State University
11935 Abercorn Street
Savannah GA, 31419
912.344.2689

10. Are you aware of similar programs in other states? If YES, which ones and how does your program differ?

We are unaware of any other University, Police Department or Federal Agency with a similar program.

11. Is the program transferable to other states? What limitations or obstacles might other states expect to encounter when attempting to adopt this program?

There are 31 Universities under the University System of Georgia's umbrella. There are more than 1000 campus police departments in the United States. These schools are located so that every region has a higher education institution within commuting distance. If the model created by the law enforcement professionals at a small university can have such an enormous impact on the backlog of digital evidence imagine the impact if this policing model were to become the state or national model. There would no longer be a shortage of technicians, nor a backlog of cases. With so many suspects asking for plea deals when confronted with digital evidence, the backlog of court cases awaiting trial is being reduced thus saving the state and county significant dollars in a tight economy.

The Armstrong State University Department's program is innovative and has positive implications for criminal case investigations on an unprecedented level. We believe that no other campus police department has had such an immediate and long term impact on so many criminal investigations for so many agencies and this is why we submit this nomination for recognition to the The Southern Legislative Conference of The Council of State Governments for the State Transformation in Action Recognition (STAR) program.