RESOLUTION NO.

A RESOLUTION AUTHORIZING THE SUBMISSION OF A GRANT APPLICATION TO THE WYOMING OFFICE OF HOMELAND SECURITY FOR THE FFY 2019 STATE HOMELAND SECURITY GRANT PROGRAM (SHSP), ON BEHALF OF THE GOVERNING BODY OF LARAMIE COUNTY, WYOMING TO REQUEST FUNDING FOR THE SHERIFF'S DEPARTMENT FOR FORENSIC OPERATIONS AND SCENE SECURITY IN THE AMOUNT OF $91,000.

FOR THE PURPOSE OF: REQUESTED FUNDS WILL BE USED TO PURCHASE A DRONE WITH ACCESSORIES (CAMERA, THERMAL IMAGING, CONTROLS, DISPLAY, MULTIPLE BATTERIES, CARRYING CASE, NIGHT OPERATIONS KIT AND A PAYLOAD DROP SYSTEM) AND A 4PC PRO SERIES MOBILE DEVICE ANALYZER. FUNDS WILL ALSO SUPPORT TRAINING AND CERTIFICATION FOR UP TO THREE USERS ON BOTH APPLICATIONS.

WITNESSETH

WHEREAS, the Wyoming Office of Homeland Security receives FFY 2019 SHSP funds from the Federal Emergency Management Agency and;

WHEREAS, the Wyoming Office of Homeland Security distributes a portion of these FFY 2019 SHSP funds to Wyoming Counties and;

WHEREAS, the Laramie County Board of Commissioners is eligible to apply for and receive FFY 2019 SHSP funds for the Sheriff's Department and;

WHEREAS, the Governing Body of Laramie County desires to participate in the Wyoming Office of Homeland Security Grant Program (SHSP) by sponsoring this grant application to assist in financing the Sheriff's Department; and

WHEREAS, the Governing Body of Laramie County has been provided with preliminary cost estimates and information on this project; and

NOW, THEREFORE, BE IT RESOLVED BY THE GOVERNING BODY OF LARAMIE COUNTY that a grant application in the amount of $91,000 be submitted to the Wyoming Office of Homeland Security for consideration of assistance in funding the Laramie County Sheriff's Department under the FFY 2019 SHSP grant program.

BE IT FURTHER RESOLVED, that Sandra Newland, or her successor in the position of Laramie County Grants Manager, is appointed as agent of the Laramie County Board of Commissioners to execute and submit applications and certifications for these funds and to receive funds and implement the programs funded under this grant.

PASSED, APPROVED AND ADOPTED THIS 16th DAY OF APRIL, 2019.

By:_____   Date: _____

Linda Heath, Chairman

ATTEST:

_____   Date: _____

Debra Lee, Laramie County Clerk

Received and Approved as to Form only By:

_____   Date: _4/9/19_____

Mark Voss, County Attorney

FFY2019 State Homeland Security Program
Grant Application

Agency Name*: Laramie County Sheriff's Department

Project Title*: Forensic Operations and Scene Security

Dollar Amount Requested*: $91,000.00

FFY2019 State Homeland Security Program
Grant Application

Applicant Information

Agency Name*: Laramie County Sheriff's Department   Type of Jurisdiction*: Law Enforcement

If other, please describe: Click here to enter text.

Legal Jurisdiction Name (if different): Click here to enter text.

Mailing Address*:   1910 Pioneer Avenue
Cheyenne, WY 82001

DUNS Number*:   197732709
*If your agency does not have a DUNS number, one can be obtained here: http://fedgov.dnb.com/webform

Agency Point of Contact (to contact in regards to this application) *: Undersheriff Rich Hillegas
Telephone Number: 307-633-4712
Email Address: rhillegas@laramiecounty.com

Alternate Agency Point of Contact (to contact in regards to this application): Sandra Newland
Telephone Number: 307-633-4201
Email Address: snewland@laramiecounty.com

Will you accept partial funding?

☒Yes
☐No

Please explain: Our request is for two projects under the realm of evidence collection and scene security. If we are partially funded we would still try to move forward with our plans on a smaller scale or only purchase one of the requested items.

Project Description

Project Justification: Community Resilience

Briefly describe the project and how it supports the investment justification.

> The Laramie County Sheriff's Department is requesting funding for a two part application that focuses on scene security and evidence collection. We are requesting funding to purchase a forensic cell phone/mobile device analyzer and a drone. This project falls under the Community Resilience section, as it provides operational support to the department. The Laramie County Sheriff's Department is requesting funding to create a drone program to serve and protect the citizens of Laramie County, Cheyenne and the surrounding areas. Our agency plans to use this equipment and training in ways that will improve officer safety, collect evidence and information and provide an effective means to address public safety issues. Drones have become an integral and effective tool for public safety agencies. Case studies have proven that the use of this technology has had a great impact on the successful resolution of a variety of incidents when deployed by first responders. Currently, this region has no access to drone technology for public safety purposes.
>
> With this proposal we are also requesting funds to procure forensic software, equipment and training which will allow the Sheriff's Department to conduct investigative operations that involve the downloading and recovery of critical evidence contained in cell phones and other mobile devices. Modern day investigations rely heavily on law enforcement's ability to obtain all available evidence that presents in a variety of ways. Evidence in digital/electronic form is especially valuable in a variety of investigations, ranging from minor property crimes to major crimes against persons or communities. This lawfully obtained information provides investigators with location, communication or photographic evidence to name a few, which are contained in mobile devices and on social media accounts.
>
> Within the 2018 Laramie County THIRA our department can contribute to addressing the core capabilities of forensics & attribution, intelligence & information sharing, physical protective measures and situational assessment through the purchase and implementation of the drone and forensic cell phone/mobile device analyzer. The county ranked operational coordination as a priority and this includes having the capability and capacity to coordinate with all agencies on scene. On scene security and protection for both citizens and law enforcement is critical to the success and efficiencies of an operation.

Describer threats and hazards that create the need.

> There are a wide spectrum of hazards and events that our request could be utilized for including manmade situations, CBRNE events, terrorist events or natural disasters. In each of these cases both the drone and cell phone analyzer could be used to provide accurate scene identification without endangering officers or other first responders. The drone in particular would create a realistic situational assessment. The forensic mobile device analyzer would provide local law enforcement officers with immediate access to equipment to conduct forensics and information sharing with all local and regional partners.
>
> Currently, the Laramie County Sheriff's Department relies on the state investigation agency to perform cell phone or mobile device forensics. We are not the only agency in the community that uses this resource, which places a burden on the state program. Leads are often delayed and evidence is sometimes lost due to the amount of time it takes to obtain this information form a single source. For the drone, the department will use the drone technology to give officers real-time, actionable intel to use while assessing the threat and formulating a strategy for their approach. It can be used to document crime scenes by providing overhead photographs and video evidence collection capabilities. Without proper equipment our department is unable to provide on scene security or operational coordination to the capabilities expected.

Explain this project's dual applicability to all-hazard events (manmade and natural hazards):

> Both the mobile device analyzer and the drone can be used on all scenes. The cause of the threat/scene is not a prohibiting factor for the equipment to be utilized. This equipment can also be a deployable asset that can be requested and used throughout the state if needed.

Identify portions of the THIRA and SPR that the project will address.

> Our request of a mobile device analyzer and drone addresses the Laramie County THIRA with examination of the operational coordination, situational assessment and on scene security, protection & law enforcement. The THIRA confirmed our known gaps in operational coordination, as the technology is continually evolving. The requested equipment would facilitate a quicker response on scene for superior mutual aid and response efforts. This equipment will also address several core capabilities to include: forensics & attribution, intelligence & information sharing,

> physical protective measures and situational assessment. Our request will help ensure a safe and secure environment to protect operations and provide decision makers with relevant information regarding the nature and extent of the hazards and maintain a unified operational structure for response.

How will this project increase capability or reduce vulnerabilities in protecting, preventing, responding, or recovering from an act of terrorism?

> The proposed project will increase our department's safety and capacity to coordinate with other officers and agencies both off and on scene. The new drone equipment will increase capabilities across the board and will reduce officer vulnerabilities. The mobile device analyzer will assist in forensic and information sharing to reduce vulnerabilities. This equipment will facilitate proper protection, prevention, and response to all scenes to include acts of terrorism. The equipment will be especially helpful in suspected terrorist events and be used for scene size up before sending in first responders.

Provide justification on how the project will be maintained, supported, and sustained.

> The Laramie County Sheriff's Department will assume all responsibility for the maintenance of the equipment to keep it operational and ready for use internally and externally by MOU partners. The requested equipment will be sustained by Laramie County for future operations. Our request would assist the Laramie County Sheriff's Department and the State in operational coordination and situational assessment.

Core Capabilities

Core Capability:
The Core Capabilities are outlined in the National Preparedness Goal which can be found at: http://www.fema.gov/pdf/prepared/npg.pdf. Additional information regarding the Core Capabilities can be found by going to http://www.fema.gov/core-capabilities. The Crosswalk of Target Capabilities can be located at http://www.fema.gov/pdf/prepared/crosswalk.pdf

Primary: **Situational Assessment**

Secondary: **On-Scene Security, Protection, and Law Enforcement**

Tertiary/Third: **Operational Coordination**

Describe existing capability levels.

> The Laramie County Sheriff's Department currently uses state resources to address the needs described above. Often times our request is put in a que and we are not able to meet our department or community threats within a reasonable time frame. This is especially true when events are affecting more than one area in the State of Wyoming. For drone capabilities, the region has no access to drone technology for public safety purposes.

Please provide an overview of the trainings, exercises, real events, or other needs assessments that have identified this as a gap (included the cause of the gap).

> The Laramie County Sheriff's Department participates in all area trainings and exercises. We have been highly involved in all planning and training efforts coordinated by our EMA office. We participate in all area exercises, trainings, table tops and planning efforts with LCCC, the refinery, CFD and the State. When we participated in the 2018 THIRA, not having adequate on scene security and forensic attribution capabilities was identified as a concern.

How will this project reduce capability gaps?

> The Laramie County Sheriff's Department will use the drone equipment and training in a variety of public safety functions; it will be used during critical incidents to locate and identify suspects who are believed to be "armed and dangerous" while personnel can maintain a safe distance. Drone technology can be used to located and identify additional evidence that cannot otherwise be seen, due to its location. The thermal technology capabilities of a drone can be used to locate actively fleeing or resisting suspects, or can be used to assist fire agencies who need to determine "hot spots" on a fire scene or when arson investigators are attempting to

determine origin and cause. The drone's payload drop capabilities can be used to deliver a cell phone to a barricaded subject during crisis negation operations. A drone's ability to give real-time video depictions of areas not accessible to first responders will improve safety, by its ability to scout an area that cannot yet be accessed due to a variety of hazardous conditions. There are many other realistic uses for drone technology in public safety, for example crowd monitoring, search and rescue and accident reconstruction to name a few. The Laramie County Sheriff's Department will find uses for this technology that will only be limited to our imagination or legal restrictions. We will cooperate with other local and regional agencies, and will provide access to the technology and agency pilots when covered by a Memorandum of Understanding.

For the mobile device analyzer it is a time critical element of evidence recovery, but analyzing large volumes of disparate data is difficult and time consuming, putting investigations at risk. The number of cases our department investigates that require this form of evidence collection, combined with frequent requests from the District Attorney's Office has made it necessary for our department to obtain the proper training and equipment to collect digital evidence more efficiently and expeditiously. The Laramie County Sheriff's Department will use this training and equipment to collect digital evidence that will generate leads and identify suspects by analyzing text, media, timeline and map information, and filter digital information to focus on the most meaningful evidence from mobile and online sources. Requests from the District Attorney's Office will also be handled in house, providing them with critical information for purposes of discovery and prosecution from a single source. Having this resource on hand will also improve our departments response to critical incidents or when working towards preventing attacks on an individual or the community.

If funded, this equipment will support our law enforcement efforts within the community and provide extended coverage and access to all first responders.

FFY2019 State Homeland Security Program
Grant Application

Basic Project Information

Primary Mission Area*: Response
Additional information regarding these Mission Areas can be found at: http://www.fema.gov/mission-areas

Does this investment focus on building new capabilities or sustaining existing?

☒ Build
☐ Sustain

Is any part of this proposed project a deployable asset? *(Identifies the availability and the utility of an asset to multiple jurisdictions, regions, and the Nation; provides information on mobility of assets in an area. An asset that is physically mobile and can be used anywhere in the United States and territories via Emergency Management Assistance Compacts (EMAC) or other mutual aid/assistance agreements)*

☒ Yes
☐ No
Please explain:

Yes, this equipment can be used as deployable asset.

Is any part of this proposed project a shareable asset? *(Identifies the asset's ability to augment and sustain a reinforced response within a region. An asset that can be utilized as a local, state, regional, or national capability, but is not physically deployable (i.e., fusion centers)*

☒ Yes
☐ No
Please explain:

This equipment can be used for multi-jurisdictional response, but is physically deployable.

Does this project support a NIMS typed resource?

☐ Yes
☒ No
Please explain:

No, the equipment is not specifically NIMS typed.

Has this project been identified as a local priority through trainings, exercises, real world events, or other needs assessments?

☒ Yes
☐ No
Please explain:

The Laramie County Sheriff's Department has prioritized this project to

assist with addressing the identified gaps within the THIRA under operational coordination, on scene security and situational assessments.

Does this project support a previously awarded investment?

☐ Yes
☒ No

If yes, what previous year, investment name and last completed milestone?

Milestones

Submit at minimum of three (3) milestones for all projects. Milestones should represent a logical progression of the project to allow for realistic monitoring and management of grant funding. This attribute will function as a tool for measuring project progress in future reporting periods. Provide a high level narrative description of activities to occur within each milestone including anticipated milestone dates/timeframes.

	Milestone/ Key activity	Projected Start Date	Projected End Date
1	Upon award, request quotes for equipment	10/1/2019	12/31/2019
2	Research equipment, evaluate quotes, award vendor contract and purchase equipment	1/15/2020	4/15/2020
3	Installation, training and implementation of equipment	05/01/2020	10/15/2020
4	Establish policies and procedures for operations	05/01/2020	10/15/2020
5	Finalize and closeout grant funds	10/15/2020	11/15/2020

1. A grant award is anticipated to occur in October 2019. At this time we will establish a budget and accounting line items to prepare for the grant. After funding has been awarded we will go out for a formal quote process according to Laramie County Procurement Policies on both pieces of requested equipment. We are anticipating this will be completed by the end of December 2019.

2. We plan on receiving quotes the beginning of February 2020 and at that time all quotes will be evaluated and a vendor recommended. We will also be conducting research on the proposed equipment for proper fit into our department. Once this process is complete we will be moving forward with our selected vendor to purchase the equipment. We are allocating three months for this process.

3. Beginning in May of 2020 we anticipate receiving the equipment. Immediately following the receipt of the equipment we will arrange for the specified training for up to three users on both items requested. We are estimating six months for this process to allow for fluctuating training schedules. At the time of the equipment arriving we will inventory and sticker all items.

4. During the same six month timeframe, the Laramie County Sheriff's Department will establish policy and procedures consistent with legal standards and applicable uses, and will establish a team of authorized pilots who will be available to deploy the drone on an as needed basis. Cooperative agreements will be established with regional agencies for the purpose of interagency cooperation in regards to the availability of drone resources. This will also be done for the authorized users of the lawful forensic evidence collection process.

5. Our final milestone will be to close out and finalize all grant items for the grant from Wyoming Office of Homeland Security. We anticipate this concluding around November 2020.

Budget Narrative

Instructions: Below you will find a budget table for each of the 5 solution areas: planning, organization, equipment, training, and exercise. Complete a budget table and narrative for each solution area associated with your project. For more information on allowable expenses for each solution area, please see the 2019 SHSP application guidance.

Budget Summary Table

Please submit the budget narrative that further details the total amount of funding being requested for each solution area.

Solution Area	Amount of Funding Requested
Planning	$0.00
Organization	$0.00
Equipment	$50,200.00
Training	$40,800.00
Exercise	$0.00
Total Amount:	$91,000.00

Planning Table

Description	Amount Requested
NO ACTIVITY	

Narrative: Summarize planned expenditures requested for planning. What is the gap identified through the THIRA/SPR being addressed? Describe how the funding will contribute to building or sustaining a core capability.

Organization Table

Description	Amount Requested
NO ACTIVITY	

Narrative: Summarize planned expenditures requested for organization. What is the gap identified through the THIRA/SPR being addressed? Describe how the funding will contribute to building or sustaining a core capability.

Equipment Table

Equipment Description	AEL Code	Requested Amount
Drone and accessories (includes camera, thermal imagining, controls and display, multiple batteries, carrying case, night operation kit, and a payload drop system.)	03SR-05-RBTL 03SR-03-SCAM	$25,000.00
4PC Pro Series CLX with licenses (2 years). Includes Universal Forensic Extraction Device (UFED) Ultimate Platform, UFED Analytics Desktop and a Cloud Analyzer.	05HS-00-FRNS 13IT-00DACQ	$25,200.00
TOTAL EQUIPMENT REQUEST:		**$50,200.00**

The AEL is available at http://www.fema.gov/authorized-equipment-list. Some equipment items require prior approval before the obligation or purchase of the items. Please reference the grant notes for each equipment item to ensure prior approval is not required.

Narrative: Summarize planned expenditures requested for equipment. What is the gap identified through the THIRA/SPR being addressed? Describe how the funding will contribute to building or sustaining a core capability.

For the first equipment request we are asking for a drone with the following accessories (camera, thermal imagining, controls and display, multiple batteries, carrying case, night operation kit and a payload drop system). The requested equipment will ensure proper functioning without limitations for usage. The drone would fall into the robotic equipment category, as it is a remotely piloted vehicle for specialized operations with an added camera. The mobile device analyzer allows for data acquisition with forensic software. Our equipment request is for a 4PC pro series CLX with licensing for two years. The device will extract, decode, and analyze logical, file system and physical data from mobile devices.

The Sheriff's Department will move forward with expenditures after a formal quote process has occurred and once a vendor has been selected. The gaps identified are situational assessment, operational coordination and on scene security, protection and law enforcement. If funded, this equipment will contribute to reducing Laramie County gaps in the mentioned core capabilities and

address the investment priorities under community resilience. We will be able to build on this core capability for future expansion and strengthening of operations.

Training Table

Training	Description	Requested Amount
Drone pilots	Training and certification for up to three drone pilots to include travel. Drone Pilot boot camp for three days includes FAA Part 107 test preparation. This test is $170 each, also includes Public Safety UAV Flight School a two day course and night operations training and waiver that is conducted online.	$25,000
Certified Logical and Physical Operator Training (forensic software)	Training and certification for up to three users including travel for a five day CCO & CCPA Certified Logical and Physical Operator training.	$15,800
TOTAL TRAINING REQUEST		**$40,800.00**

Narrative: Summarize planned expenditures requested for training. What is the gap identified through a Training and Exercise Plan or other assessment (National Emergency Communications Plan NECP Goal Assessments)? Describe how the funding will contribute to building or sustaining a core capability.

Requested training funds coincide with the equipment requested and is needed to ensure proper use and handling of equipment. For the drone it is essential for personnel who will be operating the equipment to receive certification and training. Our request is for up to three users and includes all travel necessary. After the initial training and certification process is complete, the Laramie County Sheriff's Department will seek to become a public aircraft operator agency to self-certify drone pilots for flights to perform governmental functions.

For the mobile device analyzer we are requesting training and certification for up to three users to be trained on the proper usage and operations of the forensic software for appropriate and prompt usage. Both of these training requests can be scaled down to one or two users if restrictions in funding are present.

While a gap related directly to this request was not identified through the Training and Exercise Plan, it is a critical component to implementing

the appropriate situational assessment and operational coordination of the equipment being requested. This training will provide certified operators and users of the equipment, which can also be utilized statewide or regionally if needed. This is an asset to both the Sheriff's Department and Homeland Security. This training will facilitate the building of core capabilities such as forensic attributions, intelligence and information sharing, physical protective measures and situational assessments.

Exercises Table

Exercise	Description	Requested Amount
NO ACTIVITY		

Narrative: Summarize planned expenditures requested for exercise. What is the gap identified through the Training and Exercise Plan or THIRA/SPR being addressed? Describe how the funding will contribute to building or sustaining a core capability.

FFY2019 State Homeland Security Program
Grant Application

Application Checklist

Required:
☒ Complete FFY 2019 State Homeland Security Program Grant Application
☒ NIMS Adoption Resolution
☒ THIRA/SPR Certification

If applicable:
☒ Communications maintenance and sustainment plan
☒ Training and Exercise Plan (required if funding is being requested for training or exercise)
☒ Any applicable supporting documentation (maps, product specifications, quotes, etc.)

Submit completed applications in PDF format electronically to:
Program Manager Rachel Nuss
rachel.nuss2@wyo.gov
307-777-5768

(05AU)   *Authentication Devices*

(05AU-00)   ...

05AU-00-BIOM   **Device, Biometric User Authentication**

Description:	Devices that utilize biometric characteristics (fingerprints, palm prints, retinal scanning, etc.) to authorize access to facilities and/or systems.
Applicable Grant Programs:	BZPP , EMPG , EOC , IBSGP , IBSGP , LETPA-SHSP , LETPA-UASI , MMRS , OPSG , PSGP , PSIC , SHSP , THSGP , UASI
Grant Notes:	
Applicable TCL Numbers:	2 , 5 , 6 , 7 , 8 , 10

Certain products in this category have been identified as requiring an Environmental and Historic Preservation (EHP) review. This does not apply to mobile and portable equipment, however all other items must be submitted for review. Please contact your assigned GPD Program Analyst or the Centralized Scheduling and Information Desk (CSID) at 1-800-368-6498 for further information.

05AU-00-TOKN   **System, Remote Authentication**

Description:	System used to provide enhanced remote authentication, usually consisting of a server, some synchronization scheme, and a device or token.
Applicable Grant Programs:	BZPP , EMPG , EOC , IBSGP , IBSGP , LETPA-SHSP , LETPA-UASI , MMRS , OPSG , PSGP , PSIC , SHSP , THSGP , UASI
Grant Notes:	
Applicable TCL Numbers:	2 , 5 , 7 , 8 , 10 , 28

(05EN)   *Encryption*

(05EN-00)   ...

05EN-00-ECRP   **Software, Encryption**

Description:	Encryption software for protecting stored data files or email messages.
Applicable Grant Programs:	BZPP , EMPG , EOC , IBSGP , IBSGP , LETPA-SHSP , LETPA-UASI , MMRS , OPSG , PSGP , PSIC , SHSP , THSGP , UASI
Grant Notes:	
Applicable TCL Numbers:	2 , 5 , 6 , 7 , 8 , 9 , 10 , 22 , 24 , 30 , 32

05EN-00-ETRN   **Encryption, Data Transmission**

Description:	A class of network access solutions, usually for remote access, that provide encrypted user access. May be used for remote access, point to point, or link encryption. Includes virtual private networks, and encrypted transmission modes such as SSH and SSL.
Applicable Grant Programs:	BZPP , EMPG , EOC , IBSGP , IBSGP , LETPA-SHSP , LETPA-UASI , MMRS , OPSG , PSGP , PSIC , SHSP , THSGP , UASI
Grant Notes:	
Applicable TCL Numbers:	2 , 5 , 6 , 7 , 8 , 9 , 10 , 22 , 24 , 30 , 32

(05HS)   *Host Level Security*

(05HS-00)   ...

05HS-00-FRNS   **Software, Forensic**

Description:	Application suites that allow in-depth analysis of hosts based on operating system and file systems. Software of this type may be used by law enforcement officers, government/corporate investigators and consultants to investigate the aftermath of computer-related crimes. Forensics software generally includes disk analysis tools, tools for the recovery of deleted files, and integrated database support to mark files and data of interest to investigators.
Applicable Grant Programs:	BZPP , EMPG , EOC , IBSGP , IBSGP , LETPA-SHSP , LETPA-UASI , MMRS , OPSG , PSGP , PSIC , SHSP , THSGP , UASI
Grant Notes:	
Applicable TCL Numbers:	1 , 2 , 5 , 6 , 7 , 8 , 9 , 10 , 14 , 15 , 22 , 23 , 24 , 27 , 28 , 30 , 32

05HS-00-MALW   Software, Malware Protection

Description:	Software for protection against viruses, spyware, and malicious code. May be obtained for individual hosts or for entire network segments.
Applicable Grant Programs:	BZPP , EMPG , EOC , IBSGP , IBSGP , LETPA-SHSP , LETPA-UASI , MMRS , OPSG , PSGP , PSIC , SHSP , THSGP , UASI
Grant Notes:	
Applicable TCL Numbers:	1 , 2 , 5 , 6 , 7 , 8 , 9 , 10 , 14 , 15 , 22 , 23 , 24 , 27 , 28 , 30 , 32

05HS-00-PFWL   System, Personal Firewall

Description:	Personal firewall for operation on individual workstations. Usually a software solution, but appliances are also available. See also: 05NP-00-FWAL.
Applicable Grant Programs:	BZPP , DLSGP , EMPG , EOC , IBSGP , IBSGP , LETPA-SHSP , LETPA-UASI , MMRS , OPSG , PSGP , PSIC , SHSP , THSGP , UASI
Grant Notes:	
Applicable TCL Numbers:	1 , 2 , 5 , 6 , 7 , 8 , 9 , 10 , 14 , 15 , 22 , 23 , 24 , 27 , 28 , 30 , 32

(05NP)   Network Level Security

(05NP-00)   ...

05NP-00-FWAL   Firewall, Network

Description:	Firewall (software or standalone appliance) for use in protecting networks. See also 05HS-00-PFWL.
Applicable Grant Programs:	BZPP , DLSGP , EMPG , EOC , IBSGP , IBSGP , LETPA-SHSP , LETPA-UASI , MMRS , OPSG , PSGP , PSIC , SHSP , THSGP , UASI
Grant Notes:	
Applicable TCL Numbers:	2 , 5 , 6 , 7 , 8 , 9 , 10 , 14 , 15 , 19 , 22 , 23 , 24 , 28 , 30 , 32

05NP-00-IDPS   System, Intrusion Detection/Prevention

Description:	Intrusion Detection and/or Prevention System (IDS, IPS) deployed at either host or network level to detect and/or prevent unauthorized or aberrant behavior on the network. Software and hardware (appliance) solutions exist. This replaces item 05NP-00-IDS and incorporates more recent prevention technology.
Applicable Grant Programs:	BZPP , DLSGP , EMPG , EOC , IBSGP , IBSGP , LETPA-SHSP , LETPA-UASI , MMRS , OPSG , PSGP , PSIC , SHSP , THSGP , UASI
Grant Notes:	
Applicable TCL Numbers:	2 , 5 , 6 , 7 , 8 , 9 , 10 , 14 , 15 , 16 , 22 , 24 , 28 , 30 , 32

05NP-00-SCAN   Tools, Network Vulnerability Scanning

Description:	Port scanners and other tools designed to identify security vulnerabilities on networks or individual hosts on target networks.
Applicable Grant Programs:	BZPP , DLSGP , EMPG , EOC , IBSGP , IBSGP , LETPA-SHSP , LETPA-UASI , MMRS , OPSG , PSGP , PSIC , SHSP , THSGP , UASI
Grant Notes:	
Applicable TCL Numbers:	2 , 5 , 6 , 7 , 8 , 9 , 10 , 15 , 22 , 24 , 28 , 30 , 32

Interactive versions of this list, including an integrated AEL/SEL display are available on-line at www.rkb.us.

Section 13   Terrorism Incident Prevention Equipment

(13IT)   Information Technology

(13IT-00)   ...

13IT-00-ALRT   System, Alert/Notification

Description:	Alert and notification equipment that allows for real-time dissemination of information and intelligence among responders via equipment such as cellular phones, pagers, text messaging, etc.
Applicable Grant Programs:	Amtrak , BZPP , IBSGP , IBSGP , LETPA-SHSP , LETPA-UASI , OPSG , PSGP , PSIC , SHSP , THSGP , TSGP , UASI
Grant Notes:	Fees related to telecommunications services to support the system are the responsibility of the jurisdiction and are not allowable under this item.
	When utilizing FEMA program funds to build, upgrade, enhance, or replace communications and information systems, grantees and sub-grantees should develop a comprehensive interoperable communications plan before procurement decisions are made.
Applicable TCL Numbers:	2 , 4 , 5 , 8 , 10 , 11 , 14 , 18 , 19 , 23 , 24 , 25 , 27 , 28 , 30 , 36

13IT-00-DACQ   Data Acquisition

Description:	Software for data collection and information / intelligence gathering, including data mining and search tools that support inferential analysis, including trend analysis.
Applicable Grant Programs:	Amtrak , BZPP , IBSGP , IBSGP , LETPA-SHSP , LETPA-UASI , OPSG , PSGP , SHSP , THSGP , TSGP , UASI
Grant Notes:	
Applicable TCL Numbers:	1 , 2 , 3 , 4 , 5 , 6 , 7 , 8 , 9 , 10 , 11 , 12 , 14 , 15 , 16 , 17 , 18 , 22 , 23 , 24 , 27 , 35

13IT-00-DEXC   Data Exchange and Interoperability

Description:	System or software designed to facilitate the exchange and interoperability of data on extramural or legacy systems such as databases, dispatch systems, records management systems, and other systems containing data useful in terrorism incident prevention.
Applicable Grant Programs:	Amtrak , IBSGP , IBSGP , LETPA-SHSP , LETPA-UASI , OPSG , PSGP , SHSP , THSGP , TSGP , UASI
Grant Notes:	
Applicable TCL Numbers:	1 , 3 , 4 , 5 , 6 , 7 , 8 , 10 , 12 , 14 , 15 , 16 , 19 , 23 , 24 , 27 , 29 , 35 , 36 , 37

13IT-00-DFSN   Data Fusion/Synthesis

Description:	Software, system or suite for accepting disparate inputs and producing organized information. May use multiple sensor inputs to develop a situational picture, and/or multiple inputs from different intelligence sources to create a correlated set of accessible data.
Applicable Grant Programs:	Amtrak , BZPP , IBSGP , IBSGP , LETPA-SHSP , LETPA-UASI , OPSG , PSGP , SHSP , THSGP , TSGP , UASI
Grant Notes:	
Applicable TCL Numbers:	1 , 3 , 4 , 5 , 6 , 7 , 8 , 10 , 12 , 14 , 15 , 16 , 19 , 23 , 24 , 27 , 29 , 35 , 36 , 37

13IT-00-FACE   Software, Facial Recognition

Description:	Facial recognition software for access control, identification of criminal actors (IFF), etc.
Applicable Grant Programs:	Amtrak , BZPP , IBSGP , IBSGP , LETPA-SHSP , LETPA-UASI , OPSG , PSGP , SHSP , THSGP , TSGP , UASI

Interactive versions of this list, including an integrated AEL/SEL display are available on-line at www.rkb.us.

03SR-03-LSTN   System, Listening

Description:	Seismic and acoustic listening devices and accessories for locating trapped and entombed victims not detectable by other means.
Applicable Grant Programs:	Amtrak , BZPP , LETPA-SHSP , LETPA-UASI , MMRS , OPSG , PSGP , SHSP , THSGP , TSGP , UASI
Grant Notes:	For use by specialty teams such as Search and Rescue or Urban Search and Rescue Teams.
Applicable TCL Numbers:	8 , 9 , 22 , 23 , 24 , 27

03SR-03-SCAM   Camera, Search

Description:	Void area video search camera and accessories for inspecting voids and confined spaces with limited physical access.
Applicable Grant Programs:	Amtrak , BZPP , LETPA-SHSP , LETPA-UASI , MMRS , OPSG , PSGP , SHSP , THSGP , TSGP , UASI
Grant Notes:	For use by specialty teams such as Search and Rescue or Urban Search and Rescue Teams.
Applicable TCL Numbers:	8 , 9 , 22 , 23 , 24 , 27 , 35

03SR-03-TPBM   Tape, Boundary Marking

Description:	Boundary marking tape: YELLOW Caution/RED Danger/ Incident specific (i.e., radiological, biological, chemical).
Applicable Grant Programs:	Amtrak , CCP , LETPA-SHSP , LETPA-UASI , MMRS , OPSG , PSGP , SHSP , THSGP , TSGP , UASI
Grant Notes:	
Applicable TCL Numbers:	4 , 8 , 9 , 11 , 12 , 14 , 15 , 16 , 18 , 19 , 20 , 21 , 22 , 23 , 24 , 26 , 27 , 28 , 29 , 30 , 33 , 34 , 35 , 36 , 37

(03SR-04)   Canines

03SR-04-DOGS   Canines, Search & Rescue

Description:	Search & rescue canines, related CBRNE training, protective equipment/garments, and handling accessories.
Applicable Grant Programs:	Amtrak , LETPA-SHSP , LETPA-UASI , MMRS , OPSG , PSGP , SHSP , THSGP , TSGP , UASI
Grant Notes:	
Applicable TCL Numbers:	8 , 9 , 19 , 22 , 23 , 24 , 27

(03SR-05)   Robotic Equipment

03SR-05-RBTL   Attachments/Tools, Search & Rescue Robot or Remotely Piloted Vehicle

Description:	Attachments/tools for specialized search & rescue capability such as mountable cameras (including infrared), remote manipulators, listening devices, etc. Includes repeater devices for extended remote operations.
Applicable Grant Programs:	Amtrak , BZPP , LETPA-SHSP , LETPA-UASI , MMRS , OPSG , PSGP , SHSP , THSGP , TSGP , UASI
Grant Notes:	For use only by specialty teams such as Search and Rescue or Urban Search and Rescue Teams.
Applicable TCL Numbers:	8 , 9 , 19 , 22 , 23 , 24 , 27

(03WA)   Water Operational & Search/Rescue Equipment

(03WA-01)   Water Operational Equipment

03WA-01-ALRT   Device, Alerting, Water Operations

Description:	Plastic, non-corrosive, pealess whistles.
Applicable Grant Programs:	Amtrak , CCP , LETPA-SHSP , LETPA-UASI , MMRS , OPSG , PSGP , SHSP , THSGP , TSGP , UASI
Grant Notes:	For use only by specialty teams such as Dive Teams or Swiftwater/Flood Search and Rescue Teams.

Interactive versions of this list, including an integrated AEL/SEL display are available on-line at www.rkb.us.

April 3, 2019

Wyoming Office of Homeland Security

Reference: Laramie County Sheriff's Dept. SHSP 2019 Application for Forensic Operations and Scene Security.

Communication Maintenance and Sustainment Plan

The Department will inventory and track the assignment of the equipment that is purchased with grant funds. There will be regular annual maintenance performed by technicians either through a maintenance contract or through an extended warranty. We intend to utilize the equipment as long as possible and as long as it is supported by vendors for service and parts. With proper handling and maintenance this equipment will be available for many years as a valuable asset to our department and others.

Critical Infrastructure Protection

The sworn Sheriff's Department staff is part of the critical infrastructure protection for Laramie County. They serve as the security providers for the Detention Center as well as for the courthouse and other county government buildings located at the county government complex in downtown Cheyenne. Typically, they will be the first responders should there be a security response needed in the city or county courtrooms or in the event of a critical incident in the county government complex; and typically they will be responding before law enforcement is called to, or arrives at, the complex.
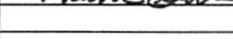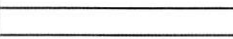
Training and Exercise Plan
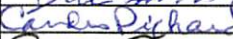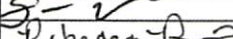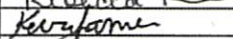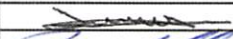
The Laramie County Sheriff's Department is requesting funding under this application for training related to the implementation of new equipment. All training and travel will follow Laramie County Policies and Procedures and certificates will be provided to Homeland Security showing proper certification. We have included costs for up to three users on both equipment requests and this includes all relevant costs pertaining to the training and certification process. The training request was not included in the Laramie County Training and Exercise Plan, but is correlating to the requested equipment specifically and meets the sustainment measurements set forth by Homeland Security.

Respectfully,

Rich Hillegas
Undersheriff

THIRA/SPR PARTICIPATION CERTIFICATION   COUNTY: LARAMIE

DATE	PRINTED NAME	SIGNED NAME	AGENCY	PHONE	EMAIL	GRANT FUNDING TYPE I.E. EMPG, SHSHP, PDM
23 Aug 18	Mikki Mensen		WOHS	779-4939	mikki.Munson@wyo.gov	
8-23-18	Dillon Conner		Laramie County Fire Dist #1	307-275-5840	dconner@LCFD1.com	
8-23-18	Darrick Mittlestadt	Dal Mttt	Laramie County Fire Dist. #1	286-4806	dmittlestadt@lcfd1.com	
8-23-18	Curtis Pickard	Curtis Pickard	Cheyenne Regional Medical Center	633-7890	Curtis.pickard@CRMCWY.ORG	
8-23-18	Sandra Newland	S-2	Laramie County, Wyoming	633-4801	snewland@laramiecounty.com	all
8-23-18	Rebecca Reid	Rebecca R	Laramie County Coroners Office	307-214-7608	Rebeccar@laramiecounty.com	
〃	Kevin James	Kevijames	Laramie County Sheriffs Office	633 4773	jamesK@laramiecounty.com	
8/23/18	NATHAN BUSZEK		CHEYENNE POLICE DEPT.	307-637-6593	NBUSZEK@CHEYENNEPD.ORG	LE
8-23-18	Susan Sweeney	Susan Sweeney	Laramie County Risk Management	307-631-5280	ssweeney@laramiecounty.com	7
8/23/18	GARY HANSON		AMR CHEYENNE/LARAMIE Cty	7704173303	Gary.Hanson@AMR.net	
8/23	Greg Hoccatt		Cheyenne Fire Rescue/Lart 7			
8.23.18	JOHN KELLEY		C-LCHD/PHRC	307-633-4063	JKELLEY@LARAMIECOUNTY 1.com	BT
8-23-18	Jeanne West		Laramie County EMA	307-633-4333	Jwest@laramiecounty.com	EMPG, SHSP
8-23-18	Matthew Butler	Matthew Butler	Laramie County EMA	307-633-4335	mbutler@laramiecounty.com	PDM, PMG

THIRA/SPR PARTICIPATION CERTIFICATION

DATE: 8-23-18

JURISDICTION/RERT #: Laramie County Sheriff's Office

PRINTED NAME: Kevin James

SIGNATURE: *Kevin James*

I certify the above by my signature, under penalty of false swearing pursuant to W.S. 6-5-303:
The Jurisdiction/RERT participated actively in a community Threat and Hazard Identification Risk Assessment (THIRA) and Stakeholders Preparedness Report (SPR) for the 2018 submission.

THIRA/SPR PARTICIPATION CERTIFICATION

DATE: _August 23, 2018_
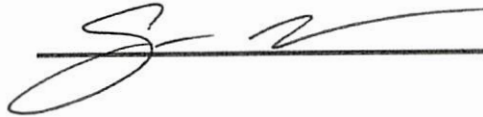
JURISDICTION/RERT #: _Laramie County, Wyoming_

PRINTED NAME: _Sandra Newland_

SIGNATURE: _[signature]_

I certify the above by my signature, under penalty of false swearing pursuant to W.S. 6-5-303:
The Jurisdiction/RERT participated actively in a community Threat and Hazard Identification Risk Assessment (THIRA) and Stakeholders Preparedness Report (SPR) for the 2018 submission.

RESOLUTION NO. 18-0320-112

'A RESOLUTION ADOPTING THE NATIONAL INCIDENT MANAGEMENT SYSTEM (NIMS), ON BEHALF OF THE GOVERNING BODY OF LARAMIE COUNTY, WYOMING

WITNESSETH

WHEREAS, the President in Homeland Security Directive (HSPD)-5, directed the Secretary of the Department of Homeland Security to develop and administer a National Incident Management System (NIMS), which would provide a consistent nationwide approach for Federal, State, and local governments to work together more effectively and efficiently to prevent, prepare for, respond to and recover from domestic incidents, regardless of cause, size or complexity;

WHEREAS, the collective input and guidance from all Federal, State, and local homeland security partners has been, and will continue to be, vital to the development, effective implementation and utilization of a comprehensive NIMS;

WHEREAS, it is necessary and desirable that all Federal, State, and local emergency agencies and personnel coordinate their efforts to effectively and efficiently provide the highest levels of incident management;

WHEREAS, to facilitate the most efficient and effective incident management it is critical that Federal, State, and local organizations utilize standardized terminology, standardized organizational structures, interoperable communications, consolidated action plans, unified command structures, uniform personnel qualification standards, uniform standards for planning, training, and exercising, comprehensive resource management, and designated incident facilities during emergencies or disasters;

WHEREAS, the NIMS standardized procedures for managing personnel, communications, facilities and resources will improve the county's ability to utilize federal funding to enhance local agency readiness, maintain first responder safety, and streamline incident management processes,

WHEREAS, the Incident Command System components of NIMS are already an integral part of various city/county incident management activities, including current emergency management training programs; and

WHEREAS, the National Commission on Terrorist Attacks (9-11 Commission) recommended adoption of a standardized Incident Command System.

NOW, THEREFORE, BE IT RESOLVED BY THE GOVERNING BODY OF LARAMIE COUNTY that the National Incident Management System (NIMS) is established as the County standard for incident management; and

BE IT FURTHER RESOLVED, that Jeanine West, or her successor in the position of Director of EMA, is appointed as agent of the Laramie County Board of Commissioners to execute and submit items and certifications for NIMS compliance.

PASSED, APPROVED AND ADOPTED THIS 20th DAY OF MARCH, 2018.

By: _K.N. Buck Holmes_
K.N. Buck Holmes, Chairman

ATTEST:

Debra K. Lee
Debra Lee, Laramie County Clerk

3-21-18
Date

Received and Approved as to Form:

_____
Mark Voss, County Attorney

3/8/18
Date

February 21st , 2018

TO WHOM IT MAY CONCERN,

This letter identifies Cellebrite as the sole developer and manufacturer of the Universal Forensic Extraction Device (UFED) Mobile Forensics solution. Cellebrite Inc., established in 1999 and based in Parsippany, NJ, is incorporated in the state of Delaware. Cellebrite Inc. supports customers and users in the US, Canada and Mexico.

The UFED is a mobile forensics extraction, decoding, and analysis tool that extracts logical, file system, and physical data from mobile devices (i.e., smartphones, cell phones, tablets, GPS units, SIM cards, memory cards, and USB devices), including live and deleted data, contacts, phone numbers, call logs, text messages, SMS messages, app data (social network and other), location data, pictures, videos, and voice messages.

UFED technology provides digital forensic lab examiners, investigators, field personnel, and first responders with the capability to collect, protect and act decisively on mobile device data with the speed and accuracy a situation demands. Our competitive advantages include:

- **Large, Established User Community.** Since 2007, Cellebrite has deployed more than 40,000 UFEDs in 100+ countries to support law enforcement, intelligence services, border patrols, military forces, public safety agencies and commercial organizations.
- **Industry's Broadest Device & App Support.** Cellebrite has established collaborative business relationships with original equipment manufacturers (OEMs) and wireless carriers worldwide. These global partners send us more than 100 new handsets per month - most prior to actual consumer market release. This allows Cellebrite Mobile Forensics to develop mobile forensics support for new devices prior to our competition. We retain more than 8,000 mobile phones at our company headquarters for ongoing innovation and support.
- **Forensically Sound Evidence Every Time.** Unlike competitors' "black box" third-party boot loaders, UFED uses custom-designed, read-only boot loaders, which ensure forensically sound file system and physical extractions
- **Technology and Research and Development (R&D) Leadership.** Cellebrite provides the mobile forensic industry's most comprehensive Android, Apple iOS, Blackberry, and Windows Mobile support. Cellebrite has a staff of 250+ engineers—the most of any mobile forensics solution provider. We are committed to investing in the ongoing R&D to innovate around customer and market needs.
- **Best-in Class Training Ensures a Repeatable, Reproducible Mobile Forensics Process.** Open to all user levels, from beginners to advanced, Cellebrite certification training provides hands-on experience with Cellebrite products and applications, delivering the tools and knowledge required for evidence collection data analysis, searching, and reporting.
- **Physical Extraction Using Bootloader Method with Lock Bypass.** Cellebrite supports physical extraction while bypassing passwords, passcodes, and pattern locks from more than 4,500 different device types, including Android (900+ devices from HTC, Huawei, LG, Motorola, and Samsung); Apple iOS; and Windows Phone (Nokia and Lumia).

UFED technology includes capabilities that are exclusive to Cellebrite and not available from any other company.

Exclusive Android Capabilities
- Decrypted physical extraction of data from Samsung Galaxy S6, Galaxy Note 5 and some Galaxy S7 devices
- Decrypting EDL - Lock-bypassing decrypted physical extraction capability for 41 Qualcomm Android devices, including Huawei H1611, Xiaomi Mi 5, ZTE Z832 Sonata 3 and ZTE Z981 ZMax Pro.
- Widely supported chipsets: 8909, 8916, 8939, 8952 and 8936
- Physical extraction and unlocking capabilities for Samsung devices! Extended support to more than 100 Exynos and

Cellebrite Inc., 7 Campus Drive, Suite 210, Parsippany, NJ 07054
Tel: (201) 848-8552 • Fax: (201) 848-9982 • www.cellebrite.com

Tax ID: 22-3770059 • DUNS: 033095568 • CAGE: 4C9Q7 • ORCA Registration Complete

Qualcomm devices including: Galaxy S7 Edge, S7, S6 Edge, S6 Edge+, Note 5, A5 and J7 families.

- Partial file system extraction while bypassing screen lock for 105 Android Samsung devices, including devices running on Android 6 OS
- Physical extraction while bypassing screen lock for 12 Samsung Galaxy S6, S6 Edge and Note 5, running on Android 6 OS
- Bootloader-based physical bypass extraction support for 48 of the toughest locked Qualcomm-based Android devices, and 33 Android devices using ADB method. This unique unlocking method supports devices based on the MSM8909, MSM8916, MSM8936, MSM8939, and MSM8952 chipsets from EDL (Emergency Download) mode. Supported Android devices include: HTC Desire: 510/620/826, Alcatel One Touch Pixi, Vivo X5/X7, Motorola XT1526 and XT1543.
- Fastest Physical Advanced ADB extractions for tested and approved 214 Android devices, including Samsung Galaxy S7, Samsung Galaxy S7 Edge, Samsung Galaxy Note 5, Samsung Galaxy S6, Samsung Galaxy Note 4, LG G4, LG G5, LG Nexus 5X, LG V20, Sony Xperia Z5, Xiaomi Redmi 3S, Huawei Nexus 6P, HTC Desire 825 and more. This capability is supported on THOUSANDS of Android devices,
- Physical extraction capability using bootloader method with lock bypass for Samsung Android devices, including Galaxy Note 4, Note Edge, S3, S4, and S5
- Lock Screen Removal (Disable User Lock) for 71 high/mid-tier Samsung Android devices. Supported devices include SM-G935T Galaxy S7 Edge, SM-J710FN Galaxy J7, SM-A700YD Galaxy A7 Duos and SM-A500W Galaxy A5
- New disable user lock capabilities have been added to 65 supported LG devices, including prepaid devices: L52VL Treasure, L15G Sunrise, LGL22C Power and LGL41C Ultimate 2
- Physical and file system ADB extractions for 51 Samsung Android devices, including SM-G935FD Galaxy S7 Edge, SM-G920T Galaxy S6 and SM-G930F Galaxy S7
- Built-in Android temporary root (granting extra permissions) for hundreds of Android devices
- Physical extraction while bypassing user lock on 140 LG devices, including the G3 and G4
- Bypass user screen lock for 137 Samsung devices, including the Galaxy S5, Tab and Galaxy Note 2, 3, and 4
- Bypass user screen lock for 17 LG devices, including the G5, new disable user lock capability for 135 LG devices including LG F700L G5, H872 G6 and US996 V20 devices.
- Physical extraction and decoding from 26 popular Motorola Android devices
- New and unique bootloader-based physical bypass extraction for 8 MTK based devices, including: Alcatel 1042x One Touch, POSH A100 Lynx and Nokia GSM 222 (RM-1136).
- Bootloader-based physical extraction from 17 MTK Android devices
- UFED User Lock Recovery Tool (Android)

Exclusive Apple (iOS) capabilities
- Decrypted physical extraction of data from Apple iPhones 4S, 5, 5c
- Full file system extraction of data from Apple devices (5/5c/6/6 plus)
- iOS unlocking support for Apple devices (4s/5/5c/6/6 plus) running iOS 8.x - 9.x, with no risk of a device wipe
- iOS unlocking support for Apple devices (5/5c/6/6 plus/7/7 plus) running iOS 10.x, with no risk of a device wipe
- UFED User Lock Recovery Tool (iOS)

Exclusive Blackberry Capabilities
- BlackBerry 10 file system extraction, backup acquisition & decryption
- Physical extraction for unlocked BlackBerry 7xxx/8xxx/9xxx devices (including NAND and NOR memory)

Other Exclusive Capabilities
- Physical extraction with password bypass for Nokia Lumia Windows Phone 8 devices, including the Lumia 520, 820, 822, 920, 928, and 1020
- Physical extraction while bypassing user lock for 3 Nokia 105 devices: RM-1133, RM-1134 and RM-1135
- Physical extraction while bypassing user lock and decoding support for 37 Huawei devices (Hisilicon)
- Physical extraction and decoding support for the latest TomTom devices, including the Go 1000 Point Trading and 4CQ01 Go 2505 Mm

Cellebrite Inc., 7 Campus Drive, Suite 210, Parsippany, NJ 07054
Tel: (201) 848-8552 • Fax: (201) 848-9982 • www.cellebrite.com

Tax ID: 22-3770059 • DUNS: 033095568 • CAGE: 4C9Q7 • ORCA Registration Complete

- Wickr app decryption (Android), TigerText app decryption (iOS)
- Provide support matrix – what is supported using username and password / application token.
- Provide traces and changes document that describe what traces the extraction process might leave.
- Supports extracting a token from the subject device in addition to the user name and password option for several of data sources including; Facebook, WhatsApp, Twitter, Gmail, Google(Location History, My Activity, Photos, Chrome, Calendar, Contacts, Drive, Bookmarks, Tasks), Mail (IMAP), Dropbox, iCloud(App, Calendar, Contacts, Drive, Photos, OneDrive, Notes, Reminder, Location), Instagram, VK, Telegram and more

Please feel free to contact Cellebrite with any questions.

Sincerely,

Gregg Weinberger
Director, Sales Operations

Cellebrite Inc., 7 Campus Drive, Suite 210, Parsippany, NJ 07054
Tel: (201) 848-8552 • Fax: (201) 848-9982 • www.cellebrite.com

Tax ID: 22-3770059 • DUNS: 033095568 • CAGE: 4C9Q7 • ORCA Registration Complete

Aaron Foy

Mimecast Attachment Protection has deemed this file to be safe, but always exercise caution when opening files.

Hi Aaron,

It was a pleasure speaking with you, as per our phone conversation below is the pricing we discussed. Please let me know if there are any questions or an official quote is needed.

UFED Platforms - https://www.cellebrite.com/en/platforms/
UFED 4PC Ultimate (includes Phone Detective, Logical and Physical Analyzer) - $9,300 includes one year of subscription the following year is $3700.

Pro Series LX includes: UFED Ultimate Platform- UFED Analytics Desktop
4PC Ultimate LX- $14,000
After the first year- license renewal fee $4,700

Pro Series CLX includes: UFED Ultimate Platform- UFED Analytics Desktop and Cloud Analyzer
4PC Ultimate CLX- $19,000
After the first year- license renewal fee $6,200

Analytics Desktop Webinar
https://vimeo.com/222668104

Analytics Desktop Video:
https://vimeo.com/224918075

Public Cloud & Analytics Desktop:
https://vimeo.com/261082015/6c2b67fcf0

Certification
https://www.cellebritelearningcenter.com/mod/page/view.php?id=16724
CCO & CCPA – Certified Logical and Physical operator
Online Certification $3290
or
5 Day class $3850
Up Coming Certifications- https://www.cellebritelearningcenter.com/local/catalog/index.php

Regards,

Janelle Vega | Regional Manager, SLED Mountain West
Desk. +1 973 206 7748 | Mobile: 973-960-4247 | e. janelle.vega@cellebrite.com | www.cellebrite.com

:.: **Cellebrite** Digital intelligence
for a safer world

Key benefits

Acquire crucial details with a forensically sound process

Fulfill requests for cloud-based private data

Gather private user data in accordance with due process from over 40 of the most popular social media and cloud-based sources, including Facebook, Twitter, Gmail, Google Drive, Dropbox, Instagram, Vkontakte, What's App, iCloud and more. Use login credentials provided by the subject, extracted from digital devices, retrieved from personal files or via other discovery means to gain access to time-sensitive evidence.

Capture public domain data for easy review

Easily access, view and incorporate publicly available data into your investigations, such as location information, profiles, images, files and social communications from popular apps, including Facebook, Twitter and Instagram.

Forensically preserve data

Log and trace the entire extraction process to maintain data authenticity. Each piece of extracted data is hashed separately and can be later compared against its origin to ensure forensic soundness and produce admissible evidence.

Enhance and share insights to accelerate investigations

Track online behavior

Gain insights into the subject's intentions, interests and relationships by analyzing posts, likes, events and connections. View text searches conducted with Chrome and Safari on iOS devices backed-up on iCloud. Extract extensive details from Google web history including private location information from a suspect or victim, so investigators can track time-stamped movements minute by minute.

Visualize data in a unified format

Bring key insights to the surface by normalizing cloud data across different sources in a unified view for easier analysis. Search, filter and examine data across platforms by Timeline, File Thumbnails, Contacts or Maps to quickly uncover common connections and correlate critical evidence.

Collaborate and integrate data

Share critical evidence with the entire investigative team. Easily generate dynamic reports that can be shared and reviewed by other team members, and export data into Cellebrite's Analytics Series or other advanced analytical tools for additional insights.

Specifications

PC	Windows compatible PC with Intel i5 or compatible running at 1.9 GHz or higher
Operating System	Windows 7 Service Pack 1, Windows 8, 64-bit or Windows 10, 64-bit
Memory (RAM)	Recommended: 16 GB / Minimum: 8 GB
Space Requirements	1.5 GB of free disk space for installation

Digital intelligence for a safer world

Digital data plays an increasingly important role in investigations and operations of all kinds. Making data accessible, collaborative and actionable is what Cellebrite does best. As the global leader in digital intelligence, and with more than 60,000 licenses deployed in 150 countries, we provide law enforcement, military and intelligence, and enterprise customers with the most complete, industry-proven range of solutions for digital forensics and digital analytics s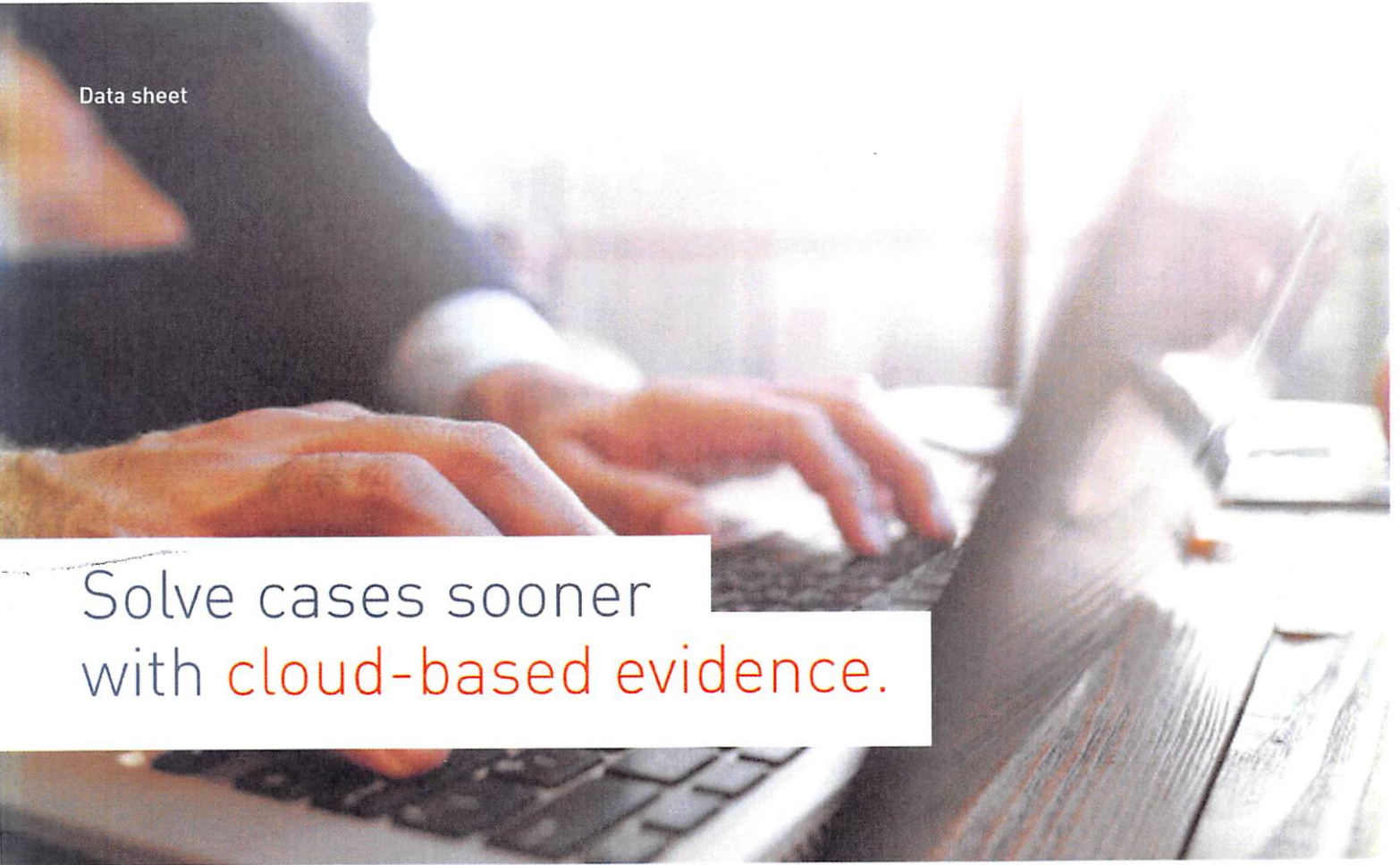olutions in the field, in the lab and everywhere in between. By enabling access, sharing and analysis of digital data from mobile devices, social media, cloud, computer and other sources, Cellebrite products, solutions, services and training help customers build the strongest cases quickly, even in the most complex situations. As a result, Cellebrite is the preferred one-stop shop for digital intelligence solutions that make a safer world more possible every day.

To learn more, visit www.cellebrite.com

Cellebrite Digital intelligence for a safer world

Solve cases sooner with cloud-based evidence.

UFED Cloud Analyzer

As people increasingly rely on social media and other cloud-based services to connect with others, store information and share their lives, digital evidence that can be critical to solving a case often exists beyond physical devices. Accessing data from public or private user profiles hosted in cloud-based applications and services needs to be fast and forensically sound to keep investigations moving forward.

Cloud-based sources represent virtual goldmines of potential evidence for investigations. But challenges abound, such as delays from service providers in meeting subpoena demands for private information after a warrant is obtained. Manually scouring public data from social media and other cloud-based apps is a time-consuming process that investigations just can't afford. Not to mention that analyzing such large volumes of disparate data presents a complex, labor-intensive challenge in and of itself. Producing timely, defensible evidence from cloud-based data has the potential to not only speed up investigations, but to crack cases wide open.

Extract, preserve and analyze social media data, instant messaging, file storage and other cloud-based content from public and legally pre-approved private sources with UFED Cloud Analyzer. Teams can immediately access insights without needing to manually comb through data or analyze an abundance of siloed information. Easily search, filter, sort and share data to quickly identify suspects, victims, locations and more.

Cellebrite Digital intelligence for a safer world

Key benefits

Recover the most data from the most devices and applications

Unlock devices with ease
Bypass pattern, password or PIN locks and overcome encryption challenges quickly and easily, giving your team access to extract and analyze its contents more quickly.

Dive deep and extract more data
Perform forensically sound advanced logical, file system and physical extractions of intact, hidden and deleted data. Our exclusive bootloaders, Advanced ADB and other recovery methods allow access to the widest variety of devices, including smartphones, feature phones, tablets, GPS devices, smart watches and more.

Decode comprehensively and quickly
Reassemble device and application data into readable formats with advanced decoding capabilities, such as Python scripting and Hex highlighting. Carve unallocated space in a device's memory to recover deleted data and media. Discover new sources of data and parse through unknown and unsupported databases by applying fuzzy methods and using the SQLite Data Wizard to reveal the greatest amount of evidence.

Reveal insights with improved processes

Unify data for more comprehensive review
Automatically consolidate data from varied sources and formats in a unified view. Focus your analysis with data searching, filtering and grouping. Identify, tag and highlight information and images against watch lists, Project VIC and other databases. View maps and timelines to determine the strength of connections between people, places and events. Translate extracted data into one language to simplify your review.

Share insights with the broader team
Further investigations by sharing key findings with the investigative team with dynamic, custom reporting that can be tailored to each colleague's specific requirements for analysis.

Platforms	
Software only	• 4PC
Mobile	• Touch2 • Ruggedized Touch2 • Ruggedized Tablet • Ruggedized Laptop

Specifications	Extraction System Requirements	Decoding System Requirements
PC	Windows compatible PC with Intel i5 or compatible running at 1.9 GHz or higher	Windows compatible PC with Intel i5 or compatible running at 1.9 GHz or higher
Operating System	Microsoft Windows 7 64-bit, 8.x 64-bit and 10 64-bit / Microsoft Windows 7 Boot Camp on Mac	Microsoft Windows 7 64-bit, 8.x 64-bit and 10 64-bit
Memory (RAM)	Recommended: 8 GB / Minimum: 4 GB	16 GB
Space Requirements	1.5 GB of free disk space for installation	1 GB of free disk space for installation

Digital intelligence for a safer world

Digital data plays an increasingly important role in investigations and operations of all kinds. Making data accessible, collaborative and actionable is what Cellebrite does best. As the global leader in digital intelligence with more than 60,000 licenses deployed in 150 countries, we provide law enforcement, military and intelligence, and enterprise customers with the most complete, industry-proven range of solutions for digital forensics, triage and analytics.

By enabling access, sharing and analysis of digital data from mobile devices, social media, cloud, computer and other sources, Cellebrite products, solutions, services and training help customers build the strongest cases quickly, even in the most complex situations. As a result, Cellebrite is the preferred one-stop shop for digital intelligence solutions that make a safer world more possible every day.

Learn more at cellebrite.com

Cellebrite
Digital intelligence for a safer world

Extract the most data sooner.
Act on intelligence quicker.
Solve cases faster.

UFED Ultimate

Complicated locks, encryption barriers, deleted and unknown content, and other data recovery obstacles can prevent critical evidence from coming to light. For investigations to get the fullest picture possible, forensic examiners and investigators need to extract forensically sound data thoroughly and quickly, and deliver meaningful insights that help advance the case.

UFED Ultimate is the market-leading solution for accessing digital forensic data, with unsurpassed capabilities to extract and decode the most data from the widest range of devices and applications. Delve deep with comprehensive access to logical, file system and physically extracted data, even hidden and deleted, and discover the critical evidence that can solve the case.

This robust, efficient tool also helps you unify collected data and review it more quickly, and easily share findings with the entire investigative team, even those not using Cellebrite products. We ensure you stay at the leading edge of digital forensic examination capabilities with the latest technology and support across a variety of hardware platforms. UFED Ultimate provides the utmost access to the data you need to build strong, defensible cases.

Cellebrite Digital intelligence for a safer world

Discover critical evidence. Solve more crimes in less time.

Analytics Desktop

When a crime occurs, the race is on to generate leads, identify suspects and make arrests. Case outcomes often rely on digital evidence, yet analyzing large volumes of disparate data is difficult and time consuming, putting investigations at risk. Forensic practitioners need fast, powerful analytics tools that can turn raw data into intelligence that investigators can act on.

Designed as a standalone application, Analytics Desktop automates time-intensive analytical tasks to deliver the deepest, most accurate insights possible and shorten investigation cycles. This cost-effective tool adds power and value to your existing forensic tools with purpose-built analytical engines that allow users to quickly correlate, analyze and cross reference large disparate sets of mobile, computer, cloud and telco data.

Dynamically view data from multiple angles and isolate key details, like objects or faces within images, for easy analysis and reporting to case stakeholders. Investigators benefit from not having to review large, cumbersome PDF reports but instead applying real-time knowledge and context required to work cases faster and keep communities safer. Prosecutors get accurate, defensible intelligence that effectively bolsters their case.

Key benefits

Reveal critical evidence faster

Text analytics

Natural language processing lets you go beyond regex and watch lists to reveal names, addresses, locations, and more from artifacts like emails, websites, text messages or even images that contain text, using OCR, in multiple languages.

Media analytics

Cutting edge machine learning algorithms immediately detect images and video related to key categories, such as weapons, nudity, faces or suspected child exploitation. Automatic facial recognition software and advanced categorization sorts data based on pre-defined filters. Identify relevant or blacklisted images by comparing digital signatures.

Timeline and map analytics

Extract location-related data from all relevant sources to track a suspect's whereabouts, identify case related hotspots and detect meetings, geo-routines and routes. Visualize mutual locations, communication flow and patterns across suspects, events or even cases, with timeline or map-based views to identify the critical connections that solve cases.

Eliminate time-intensive manual analysis

Analyze data faster

Simplify complex analytical tasks to build the case more quickly. Automatically unify and correlate data from across disparate sources, such as mobile devices, computer, cloud and telco service providers. Save time and resources by analyzing multiple logical, file system and physical extractions and external sources in various formats in a single view.

Focus on the most meaningful evidence

Eliminate the need to review images one by one with advanced media analytics utilizing unique neural network machine learning processes. Apply your case knowledge using intuitive filters to narrow your focus to the most relevant evidence. Enhance your existing forensics tools with comprehensive case-level analysis capabilities to help you advance the case.

Establish connections quickly

Dynamic visualizations help forensics practitioners and investigators uncover new perspectives and discover common threads based on communications and locations. Analyze links within case-related networks to uncover connections, group hierarchies and communication patterns between parties.

Specifications

Architecture	Recommended: Core i7 CPU / Minimum: Core i5 CPU
Operating System	Windows-based desktop
Performance Requirements	Recommended: 16+ GB RAM / Minimum: 8 GB RAM
Graphics Processing Unit	NVIDIA GPU with 2 GB of memory for image analytics
Uses/Cases	Single
Digital Artifacts	Multiple digital artifact sources (phone extraction, telco data records and UFED Cloud Analyzer extraction data per case)

Digital intelligence for a safer world

Digital data plays an increasingly important role in investigations and operations of all kinds. Making data accessible, collaborative and actionable is what Cellebrite does best. As the global leader in digital intelligence with more than 60,000 licenses deployed in 150 countries, we provide law enforcement, military and intelligence, and enterprise customers with the most complete, industry-proven range of solutions for digital forensics, triage and analytics.

By enabling access, sharing and analysis of digital data from mobile devices, social media, cloud, computer and other sources, Cellebrite products, solutions, services and training help customers build the strongest cases quickly, even in the most complex situations. As a result, Cellebrite is the preferred one-stop shop for digital intelligence solutions that make a safer world more possible every day.

Learn more at cellebrite.com

Cellebrite Digital intelligence for a safer world

Cellebrite
Digital intelligence for a safer world

UFED Cloud Analyzer provides access to private user data in accordance with due process from over 40 social media and cloud-based sources to help you acquire critical evidence.

Supported Data sources
1. Facebook
2. Telegram
3. WhatsApp (Google drive)
4. WhatsApp (iCloud backup)
5. WhatsApp (iCloud)
6. Twitter
7. Gmail
8. Google Location History
9. Google My Activity
10. Google Photos
11. Google Calendar
12. Google Contacts
13. Google Drive
14. Google Bookmarks
15. Google Search history
16. Google Tasks
17. Google Password
18. Google Account
19. Chrome – Autofill
20. OneDrive
21. Instagram
22. VK
23. Yahoo Mail (IMAP)
24. Outlook Mail (IMAP)
25. iCloud App
26. iCloud Location
27. iCloud Calendar
28. iCloud Contacts
29. iCloud Drive
30. iCloud Photos
31. iCloud Notes
32. iCloud Reminder
33. iTunes Purchases
34. Safari Search history (iCloud Backup)
35. Safari bookmark (iCloud Backup)
36. Call logs (iCloud Backup)
37. Viber (iCloud Backup)
38. Dropbox

Google Takeout (via PA)
39. YouTube (takeout)
40. Google+
41. Google Play
42. Hangouts
43. Profile
44. Keep
45. Google Fit

DSLR Pros

Drone Expert Solutions Partner

Matrice 210 - First Responder - Aerial Kit

Prepared by:
Derek Wheeler

DSLRPros.com
sales@dslrpros.com

Pricing valid for 30 days after date received

Prepared for:
Curtis Burch

Laramie County Sheriff's Office

RFQR ID: KNUUS-WVG8K-RWW9C-DWOP2
Date Created: Feb 21, 2019
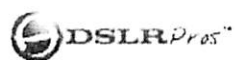
Pricing Matrix

Name	Price	QTY	SKU	Subtotal

- Uncooled VOx Microbolometer Thermal Imager
- Stabilized and Controlled by Custom DJI Gimbal
- Compatible with DJI Matrice and Inspire 1 Drones

Matrice 200 - Zenmuse XT Gimbal Adapter (Part No.8)	$149.00	1	S-DJI-M200-XT-GIM-ADAPT	$149.00

- Necessary to use Zenmuse XT with Matrice 200 Series
- Compatible with Matrice 200 Series

Zenmuse Z30	$2,999.00	1	S-DJI-Z30	$2,999.00

- 30x optical zoom
- Digital zoom up to 6x (total magnification up to 180x)
- Tap Zoom
- Stabilization Within 0.01°
- Extremely stable even when fully zoomed in
- https://www.facebook.com/DSLRPros/videos/720402891460783/

(QTY2) Matrice 200 - TB55 Intelligent Flight Battery	$738.00	2	S-DJI-M200-TB55-BATT	$1,476.00

Pair of higher capacity batteries for the Matrice 200 Series.

Estimated flight time:
- No Payload = 38 min
- X4S Gimbal = 35 Min
- X5S Gimbal = 33 min
- Z30 Gimbal = 32 min
- Z30 + XT Gimbal = 28 min
- Z30 + X5S Gimbal = 26 min

GoProfessional Cases DJI Matrice 200 Case	$739.00	1	S-GPC-M200-CASE	$739.00

Capable of safely storing everything that comes with the Matrice 200 drone and more in the custom cut foam
*** If you require the OEM case, you will need to pay additional shipping fee ***

DSLRPros offers competitive pricing and will PRICE MATCH. We offer DISCOUNTS to law enforcement agencies, emergency service organizations, government entities, educational institutions and other qualified organizations (POs are also accepted).

We offer competitive pricing and will PRICE MATCH. We offer DISCOUNTS to law enforcement agencies, emergency service organizations, government entities, educational institutions and other qualified organizations (POs are also accepted).

Subtotal	$20,110.97
First Responder Discount	-$2,050.00
Total	**$18,060.97**

Gimbal and Camera Controls

The Zenmuse XT Series Thermal Gimbal is a fully integrated FLIR Tau 2 thermal core that puts all the controls right at your fingertips.

- Spot Metering, temperature measurement at the mid-point
- Digital Zoom: x2, x4, and x8 (640 model)
- Digital Zoom: x2, x4 (336 Model)
- Single or interval shooting modes
- Photo, video preview and download
- Take photos while recording video
- Thermal Core Camera settings:
    1. Palette, also referred to as Look-up Table (LUT)
    2. Scene, also referred to as Automatic Gain Correction (AGC)
    3. Region of Interest (ROI)
    4. Isotherm mode
- Radiometric Option Available (TIFF 14-bit)
- Format: MP4, JPEG (8-bit), TIFF (14-bitRadiometric Only)

	6.8 / 7.5 mm	9 mm	13 mm	19 mm
640 x 512	90 degrees	69 degrees	45 degrees	32 degrees
336 x 256	45 degrees	35 degrees	25 degrees	17 degrees

DSLRPros offers competitive pricing and will PRICE MATCH. We offer DISCOUNTS to law enforcement agencies, emergency service organizations, government entities, educational institutions and other qualified organizations (POs are also accepted).

The DJI Pilot app is compatible with DJI FlightHub™, a web-based software package allowing teams to share real-time data with offsite parties over the Internet. This includes remote emergency situation control rooms keeping track of first response teams or asset management centers inspecting global infrastructure networks. In an easy-to-use control center, DJI FlightHub lets users plan flights with multiple drones and keep track of each aircraft's status. An offsite control room can simultaneously monitor live feeds and can remotely control gimbal and camera. The software enables managers to plan flights in advance using waypoints and dynamic geofencing.
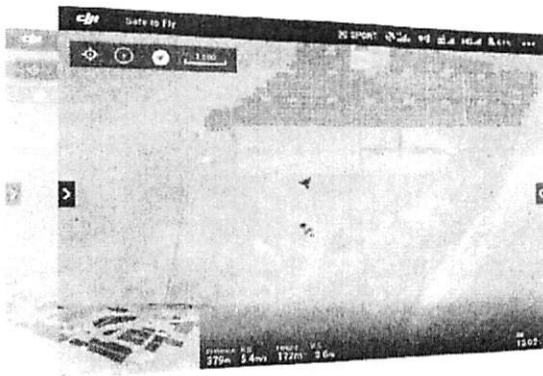
Flight Time Estimates

NO PAYLOAD — X4S · X5S · Z30 · Z30 + XT · Z30 + X5S

0.25 kg
PAYLOAD WEIGHT

23 min
EST. FLIGHT TIME BASED ON TB50

35 min
EST. FLIGHT TIME BASED ON TB55

FLIGHT TIME
Estimate your M200 Series drone's flight time based on the payload configuration.

NO PAYLOAD — X4S · X5S · Z30 · Z30 + XT · Z30 + X5S

0.46 kg
PAYLOAD WEIGHT

22 min
EST. FLIGHT TIME BASED ON TB50

33 min
EST. FLIGHT TIME BASED ON TB55

FLIGHT TIME
Estimate your M200 Series drone's flight time based on the payload configuration.

NO PAYLOAD — X4S · X5S · Z30 · Z30 + XT · Z30 + X5S

0.55 kg
PAYLOAD WEIGHT

22 min
EST. FLIGHT TIME BASED ON TB50

32 min
EST. FLIGHT TIME BASED ON TB55

FLIGHT TIME
Estimate your M200 Series drone's flight time based on the payload configuration.

NO PAYLOAD — X4S · X5S · Z30 · Z30 + XT · Z30 + X5S

0.82 kg
PAYLOAD WEIGHT

20 min
EST. FLIGHT TIME BASED ON TB50

28 min
EST. FLIGHT TIME BASED ON TB55

FLIGHT TIME
Estimate your M200 Series drone's flight time based on the payload configuration.

DSLRPros offers competitive pricing and will PRICE MATCH. We offer DISCOUNTS to law enforcement agencies, emergency service organizations, government entities, educational institutions and other qualified organizations (POs are also accepted).

Payment Options

Financing Available

Affirm financing provides innovative, technology-powered finance solutions for America's businesses as well as individuals. Basically – we're here for you so let's succeed together.

Purchase Orders

We support and welcome purchase order requisitions from local county, state and federal agencies as well as academic institutions.

Wire Transfer Method

We only recommend wire transfers for amounts over $2,000 USD.

Please contact us for information on how to complete the wire transfer to place your order.

DSLRPros offers competitive pricing and will PRICE MATCH. We offer DISCOUNTS to law enforcement agencies, emergency service organizations, government entities, educational institutions and other qualified organizations (POs are also accepted).

Drone Pilot Boot Camp

3-Day Basic Training

⊛DSLR *Pros*

Instructor Information

Instructors	LinkedIn
Brendan Stewart	https://www.linkedin.com/in/brendantstewart/
Derrick Ward	https://www.linkedin.com/in/derrick-ward-3b63128a/

General Information

Description

The drone pilot boot camp is a 3-day intensive training course to prepare new pilots for commercial UAV operations. The course includes FAA part 107 test preparation, hands-on flight exercises, and in-depth hardware training.

Expectations and Goals

Equip students with the requisite knowledge and experience to successfully pass their Part 107 aeronautical knowledge test and equip students to begin operating their UAS safely and proficiently in an emergency response capacity.

Upon completion of this course, students should be able to:

- Identify, understand and articulate the fundamental components of a successful drone program.

- Identify, understand, and comply with all federal aviation regulations pertinent to the UAS.

- Recognize classes of airspace, determine, and implement appropriate authorization procedures.

- Identify, understand, and interpret sectional charts, Chart Supplement, and airport diagrams.

- Recognize, understand, and interpret aviation weather products.

- Recognize and understand legal and physical weather limitations on the operation of the UAS.

- Recognize, understand, and implement mitigations to limit the detrimental effects of human error during the UAS operation.

- Understand and satisfactorily perform preflight inspection procedures to determine the UAS's airworthiness.

- Understand, articulate, and satisfactorily perform procedures for manual takeoffs and landings without the assistance of automated features.

- Understand, articulate, and satisfactorily perform ground reference maneuvers without the assistance of flight automation.

- Recognize and understand uncontrolled airport traffic patterns.

- Recognize and understand aviation radio communications procedures.

- Recognize, understand, and implement appropriate risk management procedures and aeronautical decision-making skills.

- Recognize, understand, and implement crew resource management and coordination procedures.

- Recognize and understand common inflight emergencies and implement appropriate management and resolution procedures.

Public Safety UAV Flight School

@DSLR Pros

2-Day Advanced Training

Instructor Information

Instructors	LinkedIn
Brendan Stewart	https://www.linkedin.com/in/brendantstewart/
Derrick Ward	https://www.linkedin.com/in/derrick-ward-3b63128a/

General Information

Description

The public safety UAV flight school is a 2-day advanced training course to prepare public safety drone pilots with specialized training for common use cases and scenarios they will encounter in the field.

Expectations and Goals

Build on the experience of proficient public safety UAV pilots through scenario-based operations focused on strategy and tactics of specific missions and large-scale deployments.

Upon completion of this course, students should be able to:

- Understand and articulate the role of the Air Operations Branch of the National Incident Management System and where the UAS team fits.

- Understand, articulate, and implement the methods and procedures to deconflict and separate multiple responding air assets; manned, and unmanned.

- Identify, understand, and implement aerial search tactics and patterns.

- Understand and implement coordination procedures between aerial and ground search teams.

- Recognize and overcome visual illusions caused by darkness and understand physiological conditions which may degrade night vision.

- Understand and implement appropriate procedures and mitigations to overcome visual illusions caused by darkness.

- Recognize and understand the effect of an external payload on the UAS' center of gravity.

- Calculate and mitigate the effect on the UAS' performance due to an external payload.

- Release external payloads from the UAS safely and effectively.

- Recognize and understand UAS search tactics and methodology.

- Develop and execute UAS search plan.

- Recognize and understand the function and theory of photogrammetric operations.

- Plan and execute a photogrammetry flight plan.

- Process, analyze, and interpret photogrammetric maps and models.

Night Operations Training & Waiver   ⊜ **DSLR** *Pros*

Online Live Training and FAA Waiver Application Service

General Information

Description

Emergencies don't stop when the sun goes down. Your team could be called to fly with a moment's notice at any time or your mission could extend far past sunset. Under Part 107, flying at night requires additional FAA approvals and training. Alternatively, if you have a Public COA with night operations, you may already have the approvals, but will need to meet the FAA's mandated training requirements for compliance and safety of flight. So, what can your agency do to fly legally & safely?

Let us manage the process with the FAA and train your pilots and visual observers to comply with your waiver.

Expectations and Goals

This training fulfills the FAA requirements for flying at night, either under a waiver of 107.29 or public COA.

- Creation, submission and approval on your agency's behalf 107.29 (night ops) waiver application.

- Training for 2 crew members to meet the FAA's night operations standards. (online live training)

    o   Visual illusions, vision anatomy, flight physiology, and human factors

    o   Flight crew roles and responsibilities

    o   Night ops best practices

- One on one support from our chief pilot to answer any questions you have along the way.

Requirements

Prerequisites

- Pilot holds a current Remote Pilot's Certificate (Part 107)

Pricing

Package	Total
2 Students + Waiver Application	$500
Additional Students	$150