



U.S. Department of Justice

Bureau of Alcohol, Tobacco,
Firearms and Explosives

I

I

www.atf.gov

January 31, 2023

FOIA Request: 2021-0948

FOIA Litigation: 22-cv-00149

VIA EMAIL: liheanachor@citizensforethics.org

Ms. Laura Iheanachor
Citizens for Responsibility and Ethics in Washington
1331 F St. NW, Suite 900
Washington, D.C. 20004

Dear Ms. Iheanachor:

This responds to your Freedom of Information Act (FOIA)/Privacy Act request dated September 13, 2021, in which you requested the following records:

1. The Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) body-worn camera (BWC) policy and phased implementation plans, as required by the June 7, 2021 memorandum from Deputy Attorney General Lisa Monaco (June 2021 DAG Memo).
2. Records sufficient to identify the designated senior official with responsibility for implementation and oversight of ATF's BWC policy, per the June 2021 DAG Memo.
3. Any related communications between ATF and DOJ concerning the following items and their inclusion in the ATF BWC policy:
 - a. The responsibilities for ATF agents to carry, operate, maintain, and secure equipment, including when to activate and deactivate BWCs.
 - b. The type(s) of BWC equipment authorized for use.
 - c. The duration of time and scope of the BWC footage preserved prior to its activation in the "buffering period."
 - d. Procedures governing the collection, storage, access, retention, use, and dissemination of ATF BWC recordings.
 - e. Procedures governing the use of BWCs by all members of ATF-sponsored task forces.
 - f. Procedures for expedited public release of recordings in cases involving serious bodily injury or death
4. The Privacy Impact Assessment and plan for annual privacy reviews relating to the use of BWCs and associated equipment, as required by the June 2021 DAG Memo.

5. All communications reflecting any consultation by ATF with the Office of Records Management for the purpose of ensuring that the ATF BWC policy is fully compliant with all recordkeeping laws, regulations, rules, policies, and guidance.
6. All communications between ATF and the Justice Management Division concerning resources required for full implementation of ATF's BWC policy.
7. All records reflecting ATF efforts to design evaluation metrics to measure the impact of its BWC policy.
8. All communications between ATF and any state or local task-force partners, alerting said task-force partners about the creation or implementation of its BWC policy.

This is **Release FIVE** of a rolling production. In response to your request, we reviewed a total of 537 pages; 102 pages were non-responsive or duplicative, 81 pages were sent to other DOJ components for consultation or referral, and 342 pages are being released in full or with redactions. Individual redactions identify the exemption pursuant to which the redacted material was withheld.

For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirements of the FOIA. *See* 5 U.S.C. § 552(c). This response is limited to those records that are subject to the requirements of the FOIA. This is a standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist. This response is the final production under this FOIA request.

If you have any questions or concerns about the information provided, please contact Antonia Konkoly at Antonia.Konkoly@usdoj.gov.

Sincerely,



Adam C. Siple
Chief, Disclosure Division

To: (b) (6)
Cc: (b) (6); (b) (6)
Vanderplow, Paul D[(b) (6)]
From: (b) (6)
Sent: Mon 7/12/2021 9:49:40 PM
Subject: RE: BWC SRT Exemption

(b) (5)

I hope this helps, feel free to call or email for any further justification.

(b) (6)
Alcohol, Tobacco, Firearms and Explosives
16009 N. 81st Street, Suite 100
Scottsdale, AZ 85260
Special Agent Project Officer-Digital Evidence Management
Technical Project Office
Special Operations Division
(b) (6)

CONFIDENTIALITY NOTICE: E-mail may contain confidential information that is legally privileged. Do not read this e-mail if you are not the intended recipient.

This e-mail transmission, and any documents, files or previous e-mail messages attached to it may contain confidential information that is legally privileged. If you are not the intended recipient, or a person responsible for delivering it to the intended recipient, you are hereby notified that any disclosure, copying, distribution or use of any of the information contained in or attached to this transmission is **STRICTLY PROHIBITED**. If you have received this transmission in error, please immediately notify us by reply e-mail,

by forwarding this to (b) (6) or by telephone at (b) (6) and destroy the original transmission and its attachments without reading or saving in any manner. Thank you.

From: (b) (6)

Sent: Monday, July 12, 2021 2:21 PM

To: (b) (6)

Cc: (b) (6) (b) (6)

Subject: RE: BWC SRT Exemption

(b) (6)

Thanks for getting this rolling.

Some questions for you:

- What are the current expectations for inclusion in this program (ie: mandates for reporting)?
- What parameters are considered when approving an exemption (just those listed or are there others)?
- What format/verbiage is requested (is the below to be used or just a rough draft)?
- What is your deadline on the exemption justification?

Thank you.

(b) (6)

From: (b) (6)

Sent: Monday, July 12, 2021 4:33 PM

To: (b) (6)

Cc: (b) (6)

Subject: BWC SRT Exemption

Good afternoon,

I am in the process of creating the Phase I BWC SOP. This will be a 6 month "trial" use of BWC's in the field, specifically the Detroit FD, Phoenix FD, and the ATF National Academy. (b) (5)

Phase II will include a 12 month process of deploying BWC's to all the ATF field divisions.

(b) (5)

Thank you in advance for your help on this!

(b) (6)

Alcohol, Tobacco, Firearms and Explosives

16009 N. 81st Street, Suite 100
Scottsdale, AZ 85260
Special Agent Project Officer-Digital Evidence Management
Technical Project Office
Special Operations Division
(b) (6)

CONFIDENTIALITY NOTICE: E-mail may contain confidential information that is legally privileged. Do not read this e-mail if you are not the intended recipient.

This e-mail transmission, and any documents, files or previous e-mail messages attached to it may contain confidential information that is legally privileged. If you are not the intended recipient, or a person responsible for delivering it to the intended recipient, you are hereby notified that any disclosure, copying, distribution or use of any of the information contained in or attached to this transmission is **STRICTLY PROHIBITED**. If you have received this transmission in error, please immediately notify us by reply e-mail, by forwarding this to (b) (6) or by telephone at (b) (6) and destroy the original transmission and its attachments without reading or saving in any manner. Thank you.

To: (b) (6), (b) (7)(C)
From: (b) (6), (b) (7)(C)
Sent: Fri 8/27/2021 12:42:59 AM
Subject: Motorola
[watchguard v300 body worn camera data sheet.pdf](#)
[V300 & CCE Market Research \(2\).pdf](#)
[v300-brochure.pdf](#)
[commandcentral-evidence-brochure.pdf](#)

(b) (6), (b) (7)(C)

Good afternoon. Please see the attached quote related to the purchase of V300 Body-Worn Camera, accessories, and Command Central Evidence (Digital Evidence Management System). I have also attached product data sheets related to the Body Worn Camera solution. Please let me know if you have any questions or need any additional information.

Thank you,

(b) (6), (b) (7)(C)

--

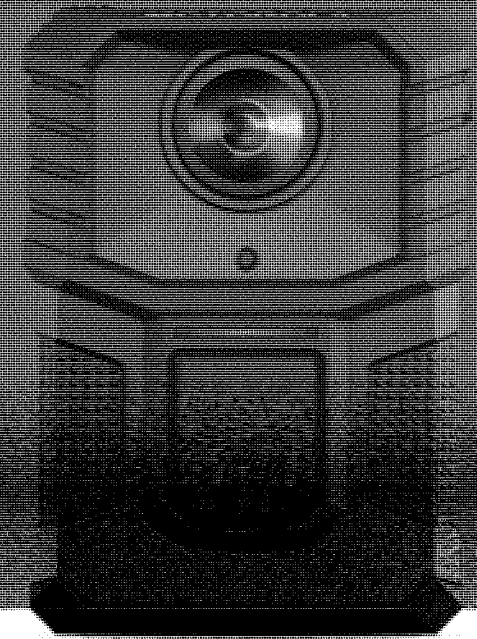
(b) (6), (b) (7)(C)
Federal Sales Manager
U.S. Federal Government Division
m: (b) (6), (b) (7)(C)



For more information on how and why we collect your personal information, please visit our [Privacy Policy](#).

V300 BODY-WORN CAMERA

Continuous-operation body-worn camera keeps officers moving forward.



KEY FEATURES

INTEGRATED WITH VEHICLE VIDEO SYSTEM

One or more V300 cameras and a 4RE® in-car system can work seamlessly as a single solution, capturing synchronized video of an incident from multiple vantage points.

AUTOMATIC WIRELESS UPLOAD

Send critical video back to headquarters while still in the field. When docked, the V300 uploads to evidence management systems via wireless networks like LTE, anytime, anywhere.

DETACHABLE BATTERY

Easily change the V300's rechargeable battery while on the go. Keep an extra battery at the ready for unexpectedly long shifts.

NATURAL FIELD OF VIEW

Eliminate the fisheye effect from wide-angle lenses that warps video footage. Distortion correction technology provides a clear and complete evidence review process.

SECURE ENCRYPTION

Elevate your data security with encryption at rest and in transit technology. V300 guards your data and your reputation.

CRITICAL EVIDENCE RECOVERY

Never miss capturing a critical incident even days after it happened and a recording wasn't activated.

SYSTEM

Temperature Range (Operational)	-20°C to +60°C; -4°F to +140°F
Field of View	130° Horizontal 73° Vertical, adjustable up + 15° down - 20° (User can adjust vertical field of view)
Dimensions	3.5 in (H) x 2.4 in (W) x 1.1 in (D); 8.9 cm (H) x 6.1 cm (W) x 2.8 cm (D)
Battery Dimensions	2.4 in (H) x 2.5 in (W) x 0.6 in (D); 6.0 cm (H) x 6.4 cm (W) x 1.6 cm (D)
Battery Weight	3.5 oz (99.2 g)
Combined Weight	6.8 oz (192.8 g)
MIL SPEC	MIL-STD-810G
Ingress Protection (IP) Rating	IP67
GPS	Yes
Bluetooth®	Yes 5.0
Wi-Fi®	802.11 n
LCD Display	Battery condition, Memory space used and available, Number of recordings, Incident categories, Current recording duration, Current time/date, Assigned officer name, covert recording status, error codes, Wi-Fi, GPS.
Activity Indicators	Multi-tone speaker, Vibration motor, Colored LED indicators.
Mounting Options	Magnetic Chest Mount Designed to fit perfectly over shirt placket buttons and zippers. MOLLE Mount Two adjacent loops across 2 rows of MOLLE webbing secures the camera to your uniform.



VIDEO RECORDING	
Resolutions	1920x1080 (1080p), 1280x720 (720p), 864x480 (480p).
Frames per second	30, 15, 10 and 5 fps (Configurable per agency requirements).
Storage Capacity	128GB / 23 hours of 1080p HD video; 46 hours of 720p HD Video; 114 Hours of 480p SD Video.
Video Compression	H.264 High Profile - reduces file sizes by nearly 50% and provides best image quality to file size ratio.
Group Recording Activation	Integrates with 4RE in-car video system and other V300 body-worn cameras. Bidirectional activation.
Dewarping	Vertical dewarping (removes fisheye effect).
Image Sensor*	4K sensor.
Pre-Event Options	None, 15s, 30s, 45s, 1m, 2m Continuous background recording also available.
Redundancy	Record-After-The-Fact

*Image sensor is 4K but is used for digital turret adjustment. Recording maximum resolution is 1080p.

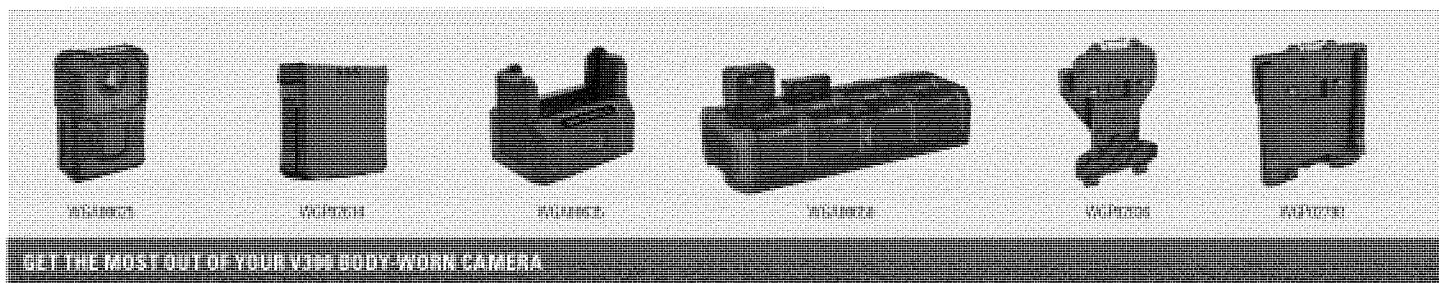
AUDIO RECORDING	
	AAC Audio.
High Quality Audio	Acoustic foam chamber blocks wind noise.
	High-tech membrane blocks water but not sound.
	Dual Audiophile quality solid state microphones, eliminate wind noise.

BATTERY	
Type	Lithium Polymer, field-swappable, rechargeable .
Stand-by	Will vary on configuration.
Charging Time	< 4 hours**.

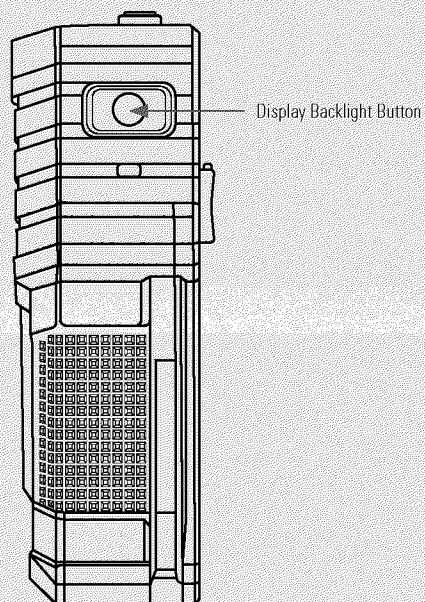
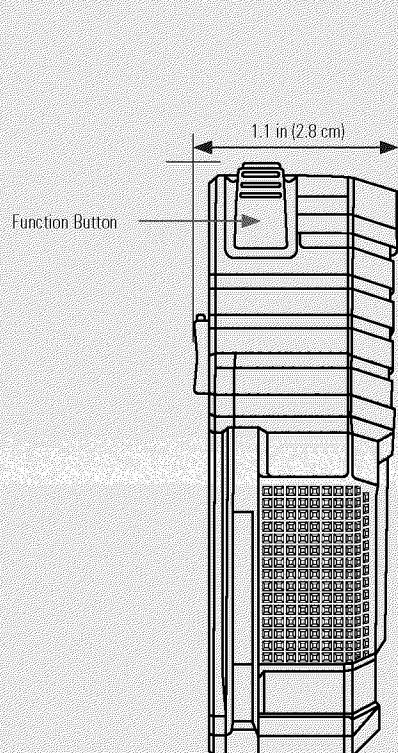
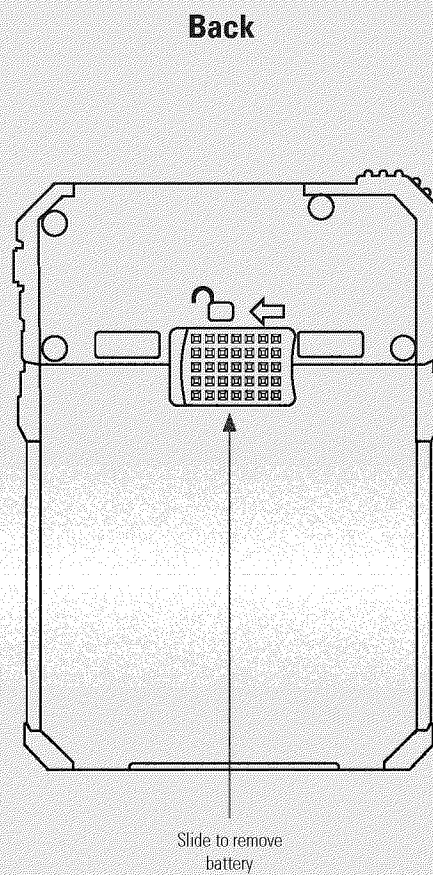
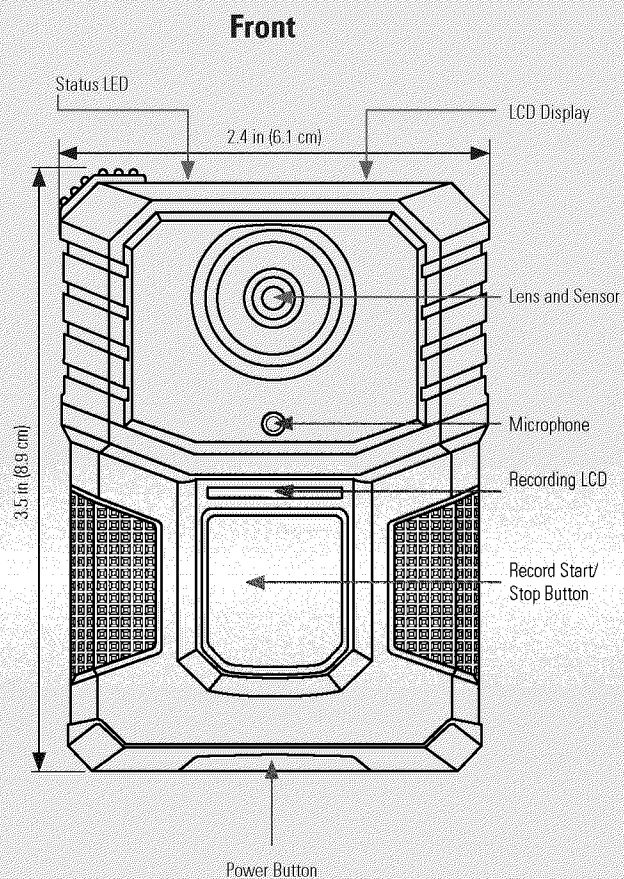
EVIDENCE MANAGEMENT	
Evidence Library	Store, manage and share evidence in a cloud-hosted or on-premises system.

**Using ethernet transfer station.

V300 CAMERA & ACCESSORIES



WGA00625	V300 Body-Worn Camera
WGP02614	Spare Camera Battery
WGA00635	Wi-Fi Camera Docking Base
WGA00650	Ethernet Transfer Station
WGP02798	Magnetic Camera Mount
WGP02836	MOLLE Camera Mount





For more information, please visit: www.motorolasolutions.com/v300

Motorola Solutions Inc., 500 W Monroe St, Chicago, IL 60661. U.S.A

Availability is subject to individual country law and regulations. All specifications shown are typical unless otherwise stated and are subject to change without notice. MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners.
© 2021 Motorola Solutions, Inc. All rights reserved.(01/21) (V13) (US)



Quote For:

ATF- Department of Justice

Attn: (b) (6), (b) (7)(C)

Reference:

V300 & CCE Market Research

Quote By:

WatchGuard Video

(b) (6), (b) (7)(C)

Date: 08-26-21

Serving Law Enforcement with the Most Compelling, Quality Video Products

FACT SHEET

MOTOROLA SOLUTIONS

Motorola Solutions is a global leader in mission-critical communications. Our technology platforms in communications, command center software, video security & analytics, and managed & support services make cities safer and help communities and businesses thrive.

We have a rich history of firsts, including pioneering mobile communications in the 1930s, making equipment that carried the first words from the moon in 1969 and developing the first commercial handheld cellular phone in 1983.

Today, our global employees are committed to designing and delivering the solutions our customers refer to as their lifeline. At Motorola Solutions, we are ushering in a new era in public safety and security.

TECHNOLOGY PLATFORMS



**MISSION-CRITICAL
COMMUNICATIONS**



**COMMAND CENTER
SOFTWARE**



**VIDEO SECURITY &
ANALYTICS**



**MANAGED &
SUPPORT SERVICES**

AWARDS

The Wall Street Journal Management Top 250,
No. 92, November 2019

WayUp Top 100 Internship Programs, August 2019

Fortune World's Most Admired Companies,
No. 3 in Networks and Other Communications
Equipment, January 2019

Forbes World's Best Employers, October 2018

Dow Jones Sustainability North American Index,
September 2018

CHAIRMAN & CEO
Greg Brown

HEADQUARTERS
500 W. Monroe
Chicago IL USA

MEDIA CONTACT

Brittany Kelly | 224-246-3914
brittnay.kelly@motorolasolutions.com

BY THE NUMBERS

\$7.3 BILLION
in annual sales (2018)

\$637 MILLION
in R&D spending (2018)

\$3.3 BILLION
in acquisitions spending since 2016

17,000+ EMPLOYEES
in 60 countries

100,000+ CUSTOMERS
in over 100 countries

6,900+ PATENTS
granted and pending

13,000 NETWORKS
across the globe



Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 U.S.A. motorolasolutions.com

MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. © 2019 Motorola Solutions, Inc. All rights reserved. 12-2019

ATF-2021-0948-RP5-000750

 MOTOROLA SOLUTIONS		WatchGuard Video 415 E. Exchange Allen, TX 75002 (P) 800-605-6734 (F) 212-383-9661			
Issued To:	ATF- Department of Justice - Attention: Christine VanWerden			Date:	08-26-21
Project Name:	V300 & CCE Market Research			Quote ID:	AYM-0004-02

PROJECT QUOTATION

We at WatchGuard Video are pleased to quote the following systems for the above referenced project:

Qty	Item #	Description
(1)	BW-V30-10--	V300, WiFi/Bluetooth Wearable Camera, with Magnetic Chest Mount <ul style="list-style-type: none"> V300, WiFi/Bluetooth Wearable Camera Magnetic Chest Mount
Subtotal Price (Excluding sales tax)		(b) (4)

Qty	Item #	Description
(1)	WGP02836	V300 CAMERA MOUNT, M330 MOLLE LOOP W/ QUICK RELEASE LEVERS
Subtotal Price (Excluding sales tax)		(b) (4)

Qty	Item #	Description
(1)	WGP02697	V300 Camera Mount; Shirt Clip rotatable
Subtotal Price (Excluding sales tax)		(b) (4)

Qty	Item #	Description
(1)	WGP02614	V300, Battery, Removable and Rechargeable, 3.8V, 4180mAh
Subtotal Price (Excluding sales tax)		(b) (4)

Qty	Item #	Description
(1)	BW-ACK-V3-TS	V300 Transfer Station II with Power Supply and Cables. <ul style="list-style-type: none"> V300 Transfer Station II TS02, D350, 8-Slot Rack Mount Charge/Upload Dock, 10GB includes kit with Power Supply and Cables.
Subtotal Price (Excluding sales tax)		(b) (4)

Qty	Item #	Description
(1)	WGA00640-KIT1	V300 Base Assembly, USB Desktop Dock
Subtotal Price (Excluding sales tax)		(b) (4)

Qty	Item #	Description
(1)	SSV00S02600A-01	CommandCentral Evidence Standard - One (1) Year Subscription <u>Offer Includes:</u> <ul style="list-style-type: none"> Digital Evidence Management Field Response Application Records Management <u>Subscription Info:</u> <ul style="list-style-type: none"> One (1) Year Subscription Duration Priced Per Named User (Qty = # of Users)
Subtotal Price (Excluding sales tax)		(b) (4)

Qty	Item #	Description
(1)	SSV00S02783A	CC Evidence Storage <ul style="list-style-type: none"> Data Storage \$0.75 per Gigabyte annually
Subtotal Price (Excluding sales tax)		(b) (4)

Qty	Item #	Description
(1)	WGW00122-410	Quick Start Software Installation Service; Remote Install, Training, Configuration, Project Management, Consultation
Subtotal Price (Excluding sales tax)		(b) (4)

Qty	Item #	Description
(1)	FRT-BWC-01	Shipping - BWC Unit <ul style="list-style-type: none"> Freight delivery for each Body Worn Camera Unit
Subtotal Price (Excluding sales tax)		(b) (4)

Qty	Item #	Description
(5)	FRT-MISC	Miscellaneous Shipping <ul style="list-style-type: none"> Freight delivery for Hardware (Parts and/or Accessories)
Subtotal Price (Excluding sales tax)		(b) (4)

Quote Notes:

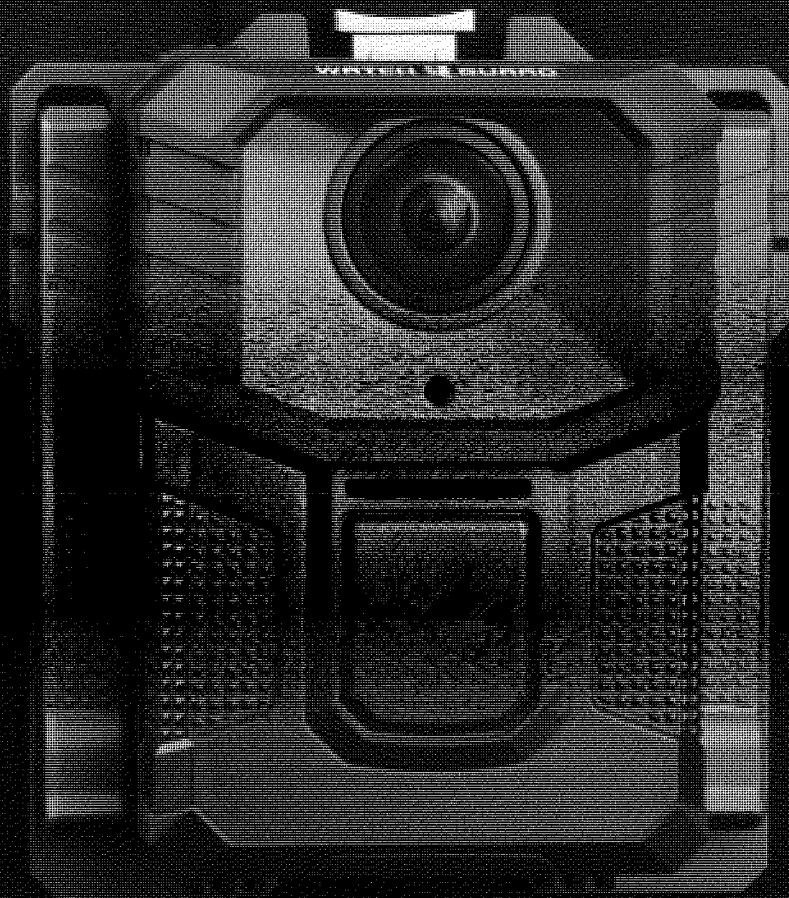
1. This Quote is valid for 90 days from the Quote Date. Pricing may change thereafter.
2. Any sales transaction resulting from this Quote is based on and subject to the applicable Motorola's Standard Terms and Conditions, notwithstanding terms and conditions on purchase orders or other Customer ordering documents.
3. Motorola's Standard Terms and Conditions are found at www.motorolasolutions.com/product-terms.
4. Payment Terms: Equipment-Net 30 days upon shipment; Installation-Net 30 days upon completion; Services and Subscription Agreements-Net 30 days from receipt of Order.

- 5. The pricing in this Quote does not include any applicable taxes (e.g. sales/use tax).
- 6. This quote is per our conversation & detail provided by you - not in accordance with any written specification.
- 7. This is a hosted service,
- 8. All hardware components to have a standard one (1) year hardware warranty.
- 9. All software to have a standard one (1) year warranty.
- 10. This quote does not included anything outside the above stated build of materials.

Quoted by:

(b) (6), (b) (7)(C) - Sr Solution Sales Representative - (b) (6), (b) (7)(C) - (b) (6), (b) (7)(C)

Total Price	(b) (4) (Excluding sales tax)
-------------	-------------------------------



WATCHGUARD V300 CONTINUOUS-OPERATION BODY CAMERA

The WatchGuard V300 continuous-operation body camera with detachable battery, wireless uploading and expansive storage addresses law enforcement's need for cameras to operate beyond a 12-hour shift.



KEY FEATURES

DETACHABLE BATTERY – Easily change the WatchGuard V300's rechargeable battery while on the go. Keep an extra battery at the ready for unexpectedly long shifts, extra shifts or part-time jobs where a body camera is required.

AUTOMATIC WIRELESS UPLOADING – Send critical video back to headquarters while still in the field. When docked in the vehicle, the V300 uploads to evidence management systems via wireless networks like LTE and FirstNet, anytime, anywhere.

INTEGRATED WITH IN-CAR SYSTEM – One or more V300 cameras and a WatchGuard 4RE® in-car system can work seamlessly as a single system, capturing synchronized video of an incident from multiple vantage points.

NATURAL FIELD OF VIEW – Eliminate the fisheye effect from wide-angle lenses that warps video footage. Our distortion correction technology provides a clear and complete evidence review process.

ABSOLUTE ENCRYPTION – Elevate your data security with encryption at rest and in transit technology. V300 guards your data and your reputation.

RECORD-AFTER-THE-FACT – Go back in time and capture video from events days after they happened, even when a recording wasn't automatically triggered or initiated by the officer. Don't rely on mere seconds of pre-event buffering to prove your case.

SPECIFICATIONS

Dimensions

2.6 x 1.1 x 3.6 in (65 x 29 x 91 mm)
W x D x H

Weight

6.8 oz (193 g)

Storage

128 GB

IP Rating

IP 67

Resolution

1080p, 720p and 480p

Microphones

Dual

Vertical Field of View

Electronic Turret +15° / - 20°

Field of View

130°

Encryption

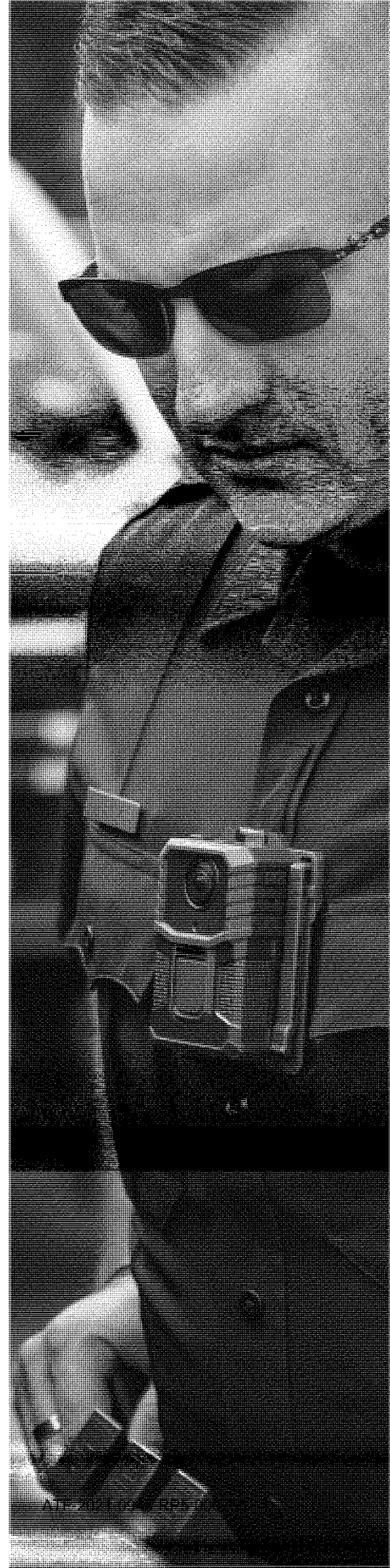
At rest and in transit

For more information, visit www.motorolasolutions.com/v300



Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 U.S.A. motorolasolutions.com

MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. © 2020 Motorola Solutions, Inc. All rights reserved. 06-2020

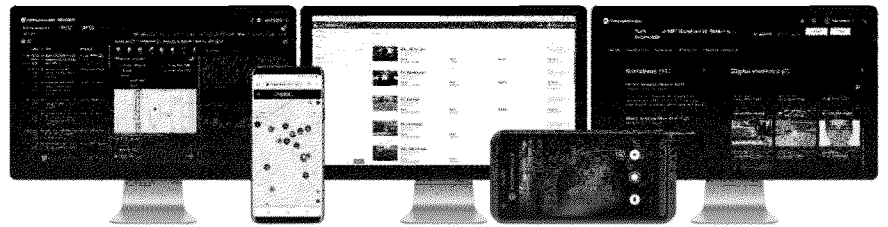


SECTION 1

COMMANDCENTRAL EVIDENCE SOLUTION DESCRIPTION

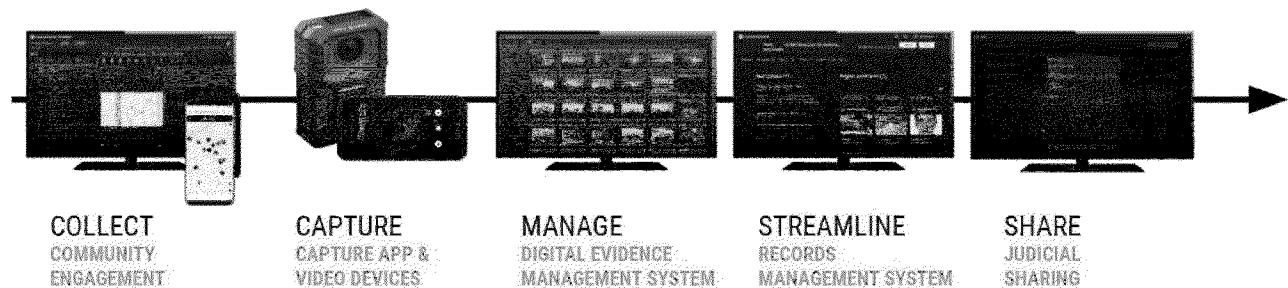
1.1 OVERVIEW

CommandCentral Evidence provides a suite of digital evidence management tools that help users contain, organize, and act on large amounts of incoming multimedia. These tools streamline the collection, capture, storage, and sharing of data from a single location. By centralizing digital evidence storage and management, CommandCentral Evidence removes data silos and helps users get the most out of their critical information.



Users access all case content from a single, cloud-based location. Cases integrate records and evidence content, allowing users to view all media associated with a case. These cloud-based tools help users account for all evidence regardless of source. CommandCentral Evidence makes it easy to secure and share content with chain of custody intact to improve collaboration.

CommandCentral Evidence is available without any upfront investment. Monthly subscription service costs include the software and video storage. And CommandCentral Evidence uses the Azure GovCloud, securing data at rest and in transit to protect communications. This complies with CJIS guidelines and the NIST framework, audited annually against the Service Organization Control 1 and 2 reporting framework.



1.2 DEVICES

CommandCentral Evidence integrates with WatchGuard video devices to help field personnel capture and upload digital evidence from the field. The included digital evidence management tools will help your agency deploy and manage these devices and manage to keep users focused on critical tasks.

1.2.1 WatchGuard V300 Body-Worn Camera

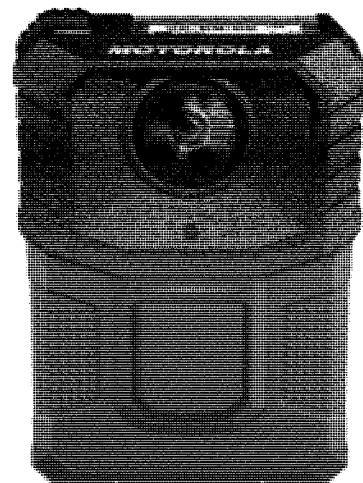
The WatchGuard V300 HD body-worn camera provides extended operation during long shifts. To support this continuous operation, officers can easily detach and swap the battery. Charged spares can remain in a docking station for a quick shift change. This enables agencies to pool camera usage by reassigning inbound cameras to outbound officers. This keeps cameras in the field, where they are most needed.

The V300 camera is easy to activate, with four control buttons and single-press recording. If an officer does not trigger a recording, the device still captures important video evidence with the Record-After-the-Fact® technology. This feature ensures important details are captured for post-incident review.

The V300 supports automatic wireless upload of video evidence, allowing officers to stay in contact from the field without distraction. The WatchGuard V300 uploads to CommandCentral Vault via a WiFi or broadband network, such as LTE or FirstNet.

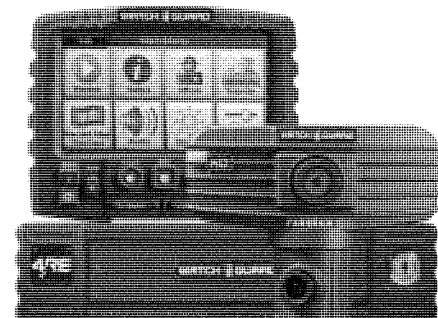
WatchGuard V300 specifications include the following:

- 4k sensor, 1080p max resolution capture, and high dynamic range.
- 128GB of memory ensures space for a full day of recorded events.
- IP67 rating for all-weather operation.
- Top backlit LCD display to view status updates on the go.
- Dual-microphone noise reduction.
- Lens distortion correction for clear video footage.
- Built-in GPS, Wi-Fi, and Bluetooth.



1.2.2 WatchGuard 4RE In-Car Video System

The WatchGuard 4RE In-Car Video System is a robust system that provides panoramic HD video coverage from a vehicle. This system integrates two cameras in a ruggedized housing. A primary camera provides normal coverage area that can be aimed as needed via a turret-mounted lense. A panoramic camera captures a wider single-camera view that is fixed in place. Together, these cameras use multi-resolution recording to capture critical event detail while on patrol.



The 4RE system features an icon-driven interface and intuitive controls to streamline field operations. Users can program various sensors to activate a new record event. These sensors include emergency lights, siren, auxiliary input, wireless microphone, vehicle speed, and crash detection. If a recording was not triggered by the user or one of these sensors, the device still captures important video evidence with the Record-After-the-Fact® technology. The system supports wireless video footage upload to CommandCentral Vault via a WiFi or broadband network, such as LTE or FirstNet.

WatchGuard 4RE specifications include the following:

- Up to 80 hours of HD video recording.
- 256 GB storage capacity.
- Certified to MIL STD 810-G standard.
- Integrated GPS and crash detection.
- Automatic Camera triggers from vehicle equipment.

1.2.3 Fully Integrated Solution

The 4RE In-Car System links with V300 body-worn cameras to create a unified video-policing system. Any camera (in-car or body-worn) can initiate a recording. Upon initiation, the other cameras will also begin recording. This feature captures an incident from multiple vantage points and synchronizes footage for playback and sharing. No one camera acts as a central controller, removing a single point of failure from the system.

The integrated system includes the body camera system, in-car system, and V300 WiFi dock. When a body-worn camera is docked in a vehicle, the device can upload data to CommandCentral Vault via broadband networks such as LTE or FirstNet. This ensures command center staff receive up-to-date information to inform better decisions.

1.2.4 Hybrid On-Premise Solution

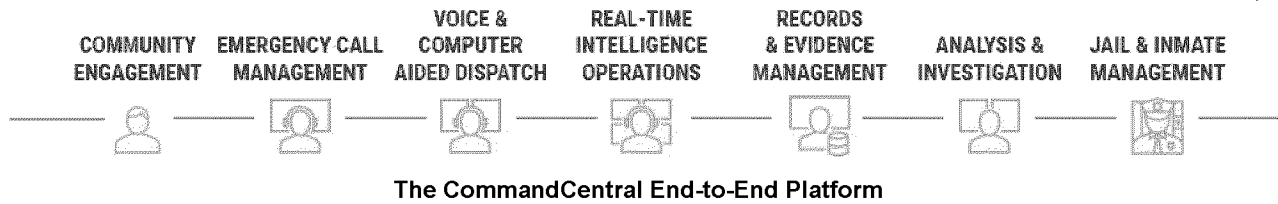
This solution includes a hybrid on-premise and cloud configuration. With this setup, your agency's on-premise Evidence Library solution will integrate with the CommandCentral cloud. This allows users to manage and share digital evidence within CommandCentral.

1.3 THE COMMANDCENTRAL PLATFORM

CommandCentral is an end-to-end platform of interconnected solutions that unify data and streamline public safety workflows from a tip or call to case closure. Through single sign-on capabilities, your personnel can access all CommandCentral software applications with one agency username and password for a more streamlined workflow. The CommandCentral platform puts your agency's data to better use, improves safety for critical personnel, and helps keep your focus on the communities you serve.

CommandCentral evolves over time, maximizing the value of existing investments while adopting new capabilities that better meet your personnel's growing needs. With cloud-based services and an agile development methodology through constant user feedback, Motorola Solutions can deliver new features and functionality in a more manageable, non-intrusive way.





1.4 COMMUNITY INTERACTION TOOLS

CommandCentral Evidence provides a set of Community Interaction tools to enhance the partnership between your agency and the public. This solution is the foundation for transparent community engagement by streamlining the flow of data between your agency and the people you serve. The toolkit helps build public trust and increases the value of community intelligence. As a result, your agency gains new ways to connect with the public, building collaboration and transparency.

Community interaction centers around CityProtect.com. This mobile-friendly webpage offers citizens a centralized set of tools to contribute to public safety. The tools and forms within CityProtect enable you to create a dialogue with your community and promote the value of citizen intelligence. Sharing and receiving important data is streamlined to make engagement easier.

Agency Page

CommandCentral Evidence provides a dedicated, public-facing webpage for your agency. This customizable page offers a unique URL to serve as the hub for community interaction with access to the tools for the public to connect with your agency.



The agency page shows quick, rotating messages—bulletins (up to five 244-character messages)—to keep the public informed. Your agency will control the order, schedule, and expiration date of these bulletins. The page also integrates an agency's social media feeds to further unify communications.

Public Submissions

With CommandCentral Evidence, the public can submit information online with an easy-to-use interface. There are multiple self-service form options for online submissions, such as anonymous tips, public information requests, and non-emergency submissions. Your agency will decide which of these forms to deploy and how to personalize these forms with built-in form management tools. The public can submit tips using these forms on CityProtect, or via anonymous SMS communication. Together, these submissions help agencies build a more accurate operating picture. TipManager manages these submissions in a central location and saves digital content in CommandCentral Evidence. This streamlines public-provided content with officer-captured evidence in a single repository.

Digital Evidence Collection

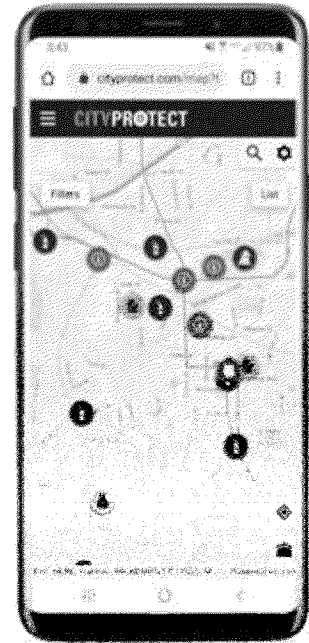
CommandCentral Evidence's digital evidence collection features allows your agency to collect case-specific digital media from any source without needing a personal device or physical storage, such as

CDs, USBs, or other devices checked into physical evidence stores. Digital files are automatically added and tagged within the application, making access to specific information easy and efficient.

Crime Map

Crime Map is built into the CityProtect home page. Crime Map automatically publishes crime data and incident information from your CAD or RMS or CAD system to an interactive, online map. This map keeps the public informed of local crime activity and offers visibility into your operations. Crime Map also provides the following:

- Incident data display with up to hourly updates.
- Primary Agency shapefile.
- Sex offender listing options.
- Crime data download option and action link.



1.4.1 Camera Registration

Camera Registration allows citizens to register their residential or commercial security cameras in CityProtect. Each community member can create a free CityProtect user account to manage their camera information. Your agency can then access the location of these cameras and contact the owner for potential video evidence. The data from these accounts is visualized in a variety of CommandCentral applications.

1.5 FIELD RESPONSE APPLICATION

CommandCentral Evidence features a mobile application that allows users to capture video, images, and audio from the field. The application provides advanced camera controls to help users control what is captured. Integrated metadata population and tagging provides immediate access of content in the Digital Evidence Management application. This isolation ensures evidence is not accessible by other apps and ensures an uncompromised chain of custody from the moment of capture.

This application is a capture source for officers, detectives, command staff, supervisors and other law enforcement personnel. The application's user interface exists in the same ecosystem as the Digital Evidence Management tool. The field response application is available on iOS and Android.

1.6 RECORDS MANAGEMENT

CommandCentral Evidence's record management capabilities allow users to quickly and easily search video, audio, images, and other digital content. It then stores that data in a central cloud-based location, streamlining access and management across your organization to reduce the complexities of record management. As a result, this solution helps save your personnel valuable time and allows them to focus on critical tasks.

Records Management offers users the following features to benefit management workflows:

- Consolidated Record View – Enter and view incident data, officer narrative, and digital evidence with one user interface, allowing officers to spend more time in the field.

- Task Creation and Assignment – View, create, and assign tasks or projects for the day as part of the Insights Dashboard. This helps build and close cases faster by tracking progress and assigning ownership to activities.
- Unified Search – Find specific information faster by searching across all agency data.
- Master Indexes – Validate data on persons, vehicles, and organizations against the master indexes. For example, agencies can verify that an arrested person, person of interest, or suspect's information is accurate.
- Compliance Verification – Prompt officers for the information they need so you can check reports before submission and save response time.
- Record Quality Control – Keep data clean by identifying, merging, and de-duplicating records automatically.
- Trusted Agency Sharing – Remain in control of your data when you share case information with other agencies.
- Judicial Case Sharing – Share validated evidence items with trusted judicial partners for use in court, with a verifiable chain of custody.
- Crime Predictions in Dashboard – Monitor activity and set threshold alerts to identify and address crime trends.
- Data Insights Reporting – Access critical insight with pre-built reports and dashboards to make data-driven decisions.

1.7 DIGITAL EVIDENCE MANAGEMENT

CommandCentral Evidence's digital evidence management tools streamline collecting, securing, and managing multimedia evidence. These tools simplify how a secure digital evidence library is built by incorporating data from multiple sources into a unified evidence storage framework. Users can upload digital evidence from a variety of sources to quickly build cases. Evidence stored within the tool is easy to search, correlate, and review alongside other case-related information from your CAD or RMS database. Relevant content can be marked and intelligently sorted to quickly locate critical information from a central touchpoint. This unified storage framework allows personnel to make informed decisions from an organized and complete case evidence view, while offering an access control system to allow only authorized personnel to view sensitive information.

1.7.1 Store and Manage

CommandCentral Evidence simplifies building a secure digital evidence library by incorporating data from multiple sources into a unified evidence storage framework. Users can upload digital evidence files from a variety of sources to build cases. Products from Motorola Solutions, such as body-worn cameras, in-car cameras, the mobile field response application, and other CommandCentral software, automatically transmit data to Digital Evidence Management. This saves the time and effort needed to manually upload files. Once the content is securely stored, content management is more efficient.

Digital Evidence Management streamlines content management workflows, with tags and metadata that make it easier to correlate, search, and manage evidence. The application automatically links evidence based on the tags and metadata attached to those files, helping users find additional contextual information on an incident and build cases quickly. Users can search and filter content to locate additional relevant data to link to a case or incident. To quickly access evidence items that they frequently need to reference, users can group or bookmark files within the interface.

CommandCentral Evidence provides unlimited storage for events captured by the WatchGuard V300 where the applied data retention period does not exceed one year for non-evidentiary recordings or 10 years for evidentiary recordings (recordings associated with a case). Additionally, the video recording

policy must be event-based (policies that require officers to record their entire shift will not qualify for this plan). For non-camera data storage (data not captured by the body camera and/or in-car system), agencies receive 50GB of storage per device, per month, pooled across all devices in the program.

CommandCentral Evidence provides unlimited storage for events captured by the WatchGuard 4RE system where the applied data retention period does not exceed one year for non-evidentiary recordings or 10 years for evidentiary recordings (recordings associated with a case). Additionally, the video recording policy must be event-based (policies that require officers to record their entire shift will not qualify for this plan). For non-camera data storage (data not captured by the body camera and/or in-car system), agencies receive 50GB of storage per device, per month, pooled across all devices in the program.

1.8 OPTIONAL INTERFACE

CommandCentral Evidence includes an optional interface that uses different mechanisms (DB polling, REST, file polling) to extract required data fields. The interface maps data fields to a corresponding format accepted by CommandCentral Evidence, and sends them to the respective applications service.

Please see the pricing section for the specific interfaces included in this proposal.

1.8.1 Interface Server Requirements

A customer-provided virtual machine is required to support the interface. The virtual machine must meet the following minimum specifications:

- 2 vCPU.
- 8GB RAM.
- 40GB Hard Drive.
- VMWare 5.5U2 1 CPU License or Hyper-V License.
- Access to Customer-Provided Internet.

The customer-provided virtual machine will allow CloudConnect to be installed to enable CommandCentral cloud applications to connect to on-premises applications, like CAD/RMS systems.



CAPTURE EVERY ENCOUNTER

THE V300 BODY-WORN VIDEO SOLUTION

ENHANCE SAFETY, TRANSPARENCY AND COMMUNITY TRUST

Police officers go above and beyond the call of duty. They need equipment that does the same. Built specifically for law enforcement, the V300 continuous-operation body-worn camera is ready to go when you are with its detachable battery, 128GB of storage space, wireless uploading and Record-after-the-Fact™ technology.

Integrated with the technology you use day in and day out to enhance your focus, and combined with powerful device and evidence management software, the V300 body-worn video solution enables you to capture every encounter.





KEEP GOING. YOUR CAMERA WILL TOO.

In a world full of cellphones and connected video devices, sometimes the only reliable witness to an incident is one you carry with you each day. Make sure it's always ready. The V300 continuous operation body-worn camera remains operational well beyond a 12-hour shift, capturing crystal clear video and audio of every encounter from the perspective that matters most.

DETACHABLE BATTERY

Easily change the V300's rechargeable battery while on the go. Keep an extra battery at the ready for unexpectedly long shifts, extra shifts or part-time jobs where a body-worn camera is required.

BUILT-IN DISPLAY

A clear LCD display on the top of the camera allows easy viewing of device status.

RUGGED & DURABLE

Tested ruthlessly to survive in a public safety environment, the V300 is shockproof, and waterproof to IP67.

AUTOMATIC WIRELESS UPLOADING

Send critical video back to headquarters while still in the field. When docked in the car, the V300 body camera uploads to cloud-based or on-premise evidence management systems via wireless networks like LTE and FirstNet, anytime, anywhere.

NATURAL FIELD OF VIEW

Eliminate the fisheye effect from wide-angle lenses that warps video footage. Our distortion-correction technology provides clear and complete video evidence.

ABSOLUTE ENCRYPTION

Elevate your data security with encryption at rest and in transit. The V300 guards your data and your reputation.

RECORD-AFTER-THE-FACT

Go back in time and capture video from events days after they happened, even when a recording wasn't automatically triggered or initiated by the officer.



EXPERIENCE REAL-TIME COLLABORATION BETWEEN DEVICES

Seamlessly integrate footage captured on V300 body-worn cameras with your 4RE system in the field, to gather indisputable evidence of any incident. Protect officers from the moment they leave the vehicle with a body-worn camera designed for shift-long wear, immediate response and in-field offload.

RADIO INTEGRATION

Reduce the officer's workload in stressful moments. When paired with APX radios via Bluetooth®, the V300 will automatically start a recording when the radio enters emergency mode, either from an officer pressing the emergency button on the radio, or from a radio-initiated "man down" event.

4RE IN-CAR VIDEO SYSTEM INTEGRATION

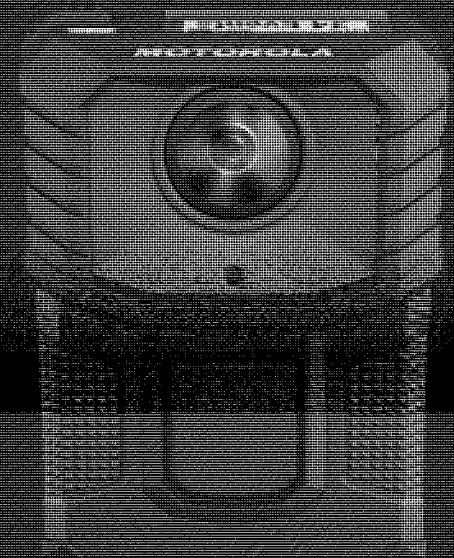
Seamlessly integrate footage captured on V300 body-worn cameras with your 4RE system in the field, to gather indisputable evidence of any incident. Protect officers from the moment they leave the vehicle with a body-worn camera designed for shift-long wear, immediate response and in-field offload.

VEHICLE INTEGRATION

Even if you don't have a 4RE, you can integrate the V300 with your vehicle to trigger a recording automatically, for example when a door is opened, a speed is exceeded, or the lights and siren are activated.

SMARTPHONE INTEGRATION

Complete your desk jobs while you're still out on patrol. The SmartControl companion app enhances your V300 body camera with a powerful toolset. Using your Android™ smartphone, you can review and tag videos, change camera settings, and view live video. Stay efficient with SmartControl.



TAKE BACK TIME WITH STREAMLINED DEVICE & EVIDENCE MANAGEMENT

PLUG INTO AN END-TO-END DIGITAL EVIDENCE MANAGEMENT SOLUTION

Managing the influx of video, images, audio and other content from a variety of different systems can cause a lot of strain for your team. But now, more than ever, this content is vital to accomplishing the right criminal justice outcomes. CommandCentral Evidence is a unified evidence management solution that enables you to aggregate and intelligently organize all of your agency's digital content in one place.

As part of CommandCentral, the industry's most integrated end-to-end public safety software suite, CommandCentral Evidence is powered by our Platform that unifies voice, video, data and analytics – ensuring information moves faster and operations are more effective.

KEY FEATURES

CASE CORRELATION

Intelligent correlation to computer-aided dispatch (CAD) and records management system (RMS) data facilitates faster review of case evidence, alleviating the burden of manually compiling evidence.

UNIFIED SEARCH

Centralizing agency data makes it easier to find the information you need with a Google-like, free text search. You can even save frequent searches so they dynamically update with any new content.

FRAME-BY-FRAME ANALYSIS

Step through video evidence frame-by-frame with granular playback control. You can control the speed of the video, step forward or backward one frame, and preview thumbnails along the video player bar to easily locate the exact video frame you need.

SYNCHRONIZED PLAYBACK

Automatically link video and audio captured by the integrated in-car and body camera system on scene, and then synchronize playback so recorded video and audio from multiple devices can be seen and heard simultaneously.

NATIVE REDACTION

Automated, intuitive redaction, available directly within CommandCentral, helps quickly protect personally identifiable information, without having to leave the application.

VIDEO TRANSCRIPTION

Easily find the information, object, vehicle or person you are looking for with automated video transcription. The video is viewable alongside the transcription, and clicking on sections of the transcript will take you to the corresponding section of the video. The transcript is searchable, and can be downloaded for court use, saving valuable time.

CASE SHARING

Quickly and securely share case content with the community, other agencies and prosecutors, as well as within your own agency. Share select media or the entire case with a case specific link via email. Download content and audit logs to make use of the systems you already have in place. Or make use of our dedicated prosecutor experience, so judicial partners can access all content shared with them – even from multiple agencies – from one, secure location.

BODY CAMERA USAGE INSIGHTS

Dive deeper into your body camera program with CommandCentral Reporting's built-in reports and dashboards. These reports provide insight into body camera usage and adoption, such as average video length and volume, policy compliance, officer behavioral changes and storage consumption to help estimate future storage needs.



EASILY CONFIGURE & ALLOCATE DEVICES

Beyond evidence management, CommandCentral Evidence makes it simple to manage your fleet of cameras. Save individual preference settings such as volume level, screen brightness and field-of-view adjustment, and apply them to future device check outs for that officer. Body-worn cameras can also be easily deployed with a Rapid Check-out Kiosk. A camera can be returned at the end of one shift, electronically reassigned and immediately checked out with a spare battery pack to another officer who is starting the next shift.

STREAMLINE YOUR DIGITAL EVIDENCE WORKFLOW

Knock down the data silos between your teams and tools with the confidence that every detail has been captured and no evidence left behind. In addition to robust, source-agnostic digital evidence management software, CommandCentral Evidence also includes community interaction tools, a secure field response application, and integrated records and evidence management. From citizen to courtroom, intuitively collect, capture, manage and share all case content through one pane of glass that centralizes all evidence types for improved accuracy and collaboration.

STILL WANT TO KEEP DATA ON-PREMISES?

Motorola Solutions offers cloud, on-premises and hybrid deployments for your specific digital evidence management requirements. For agencies that prefer to store digital evidence data on-site, Evidence Library is available as an on-premises digital evidence application. Alternatively, adopt a hybrid model to utilize the advanced cloud functionality of CommandCentral Evidence, while still storing the data on-premises.

GET THE MOST OUT OF YOUR SOLUTION

SERVICES THAT KEEP YOUR SYSTEM WORKING SO YOU CAN KEEP MOVING

INSTALLATION SERVICES

Ensure peak system performance with our site and remote installations services, such as project management, installation, configuration, inspection and testing.

TRAINING & SUPPORT

Maximize operational efficiency with on-site and online training of officers and system administrators. When you need technical support, our certified engineers use the right escalation procedures to bring you a prompt resolution.

HARDWARE WARRANTY

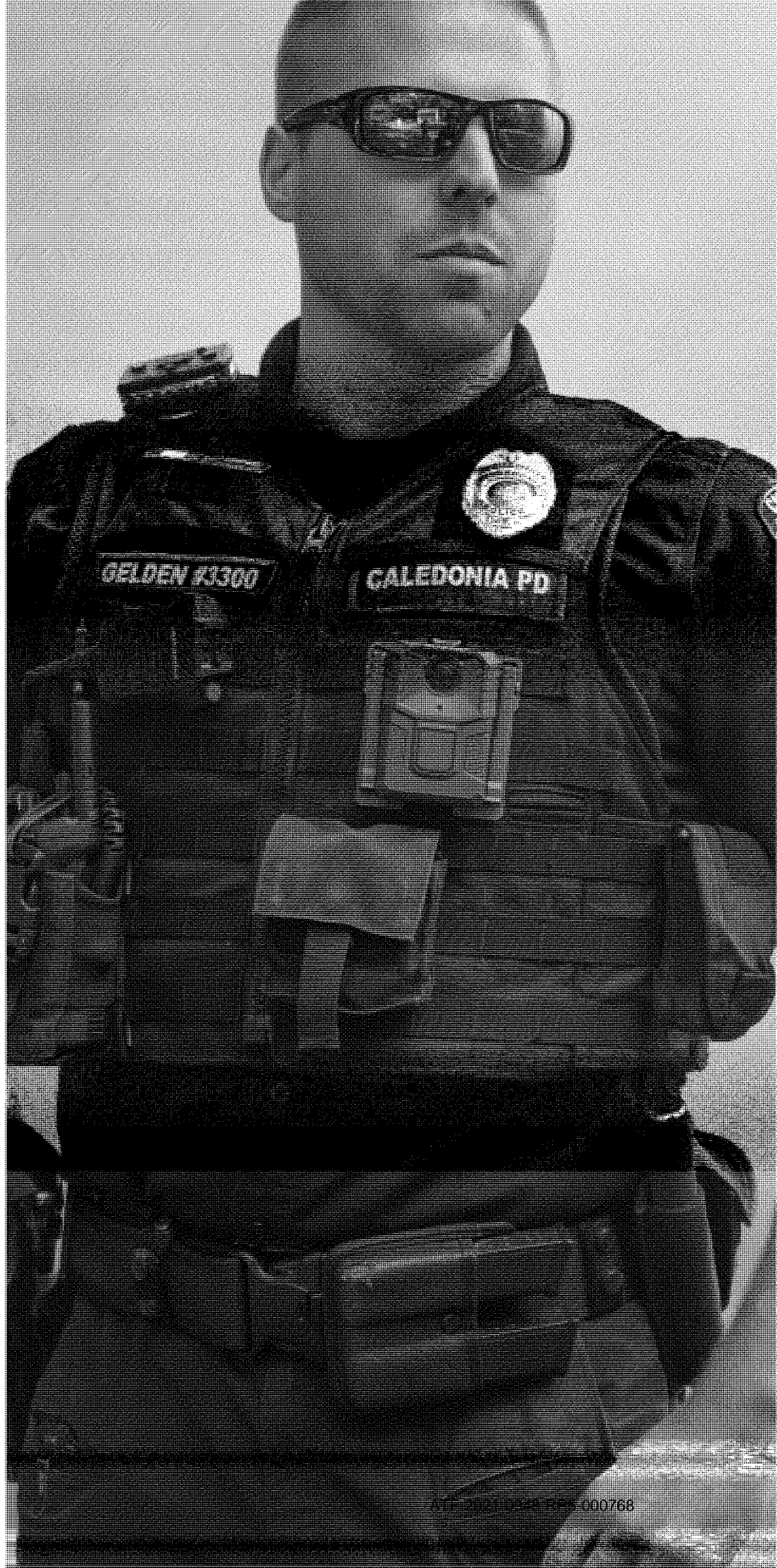
Maintain efficiency and reliability with a one, three or five-year hardware warranty plan with the option to add "no-fault" coverage at a premium.

CAMERA FIRMWARE UPDATES

We are committed to the continual testing and improvement of our firmware. As new revisions become available, these updates will be made available to your agency; fees may apply depending on your licensing agreement.

SOFTWARE MANAGEMENT & MAINTENANCE

With CommandCentral software in the cloud, enjoy automatic updates that push new features to you hassle-free. We also offer support for updates to on-prem software deployments.



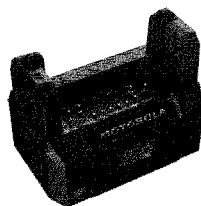
CAMERA ACCESSORIES FOR A SOLUTION THAT WORKS THE WAY YOU DO



WGA00640

USB DOCKING BASE

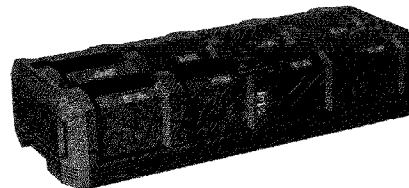
Officers working remotely can easily offload video footage from their camera by plugging the USB docking base into their computer. Upload requires the V300 USB Service for Windows PC, which can be downloaded from the USB dock webpage.



WGA00635

WIFI CAMERA DOCKING BASE

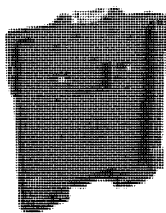
Mounted in your patrol vehicle, this dock contains a WiFi access point to connect body-worn cameras and 4RE in-car cameras in a group recording network. Placing a camera into the dock will also upload content through the car's network.



WGA00650

ETHERNET TRANSFER STATION

A high-capacity charging and offload solution, this dock allows eight cameras and batteries to be charged simultaneously, with a fast ethernet connection for rapid uploading of content. Multiple transfer stations can be interconnected.



WGP02798

MAGNETIC CAMERA MOUNT

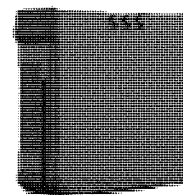
Your camera needs to be stable and securely mounted to be effective. This mount uses powerful magnets and quick-release levers to grip your uniform tightly.



WGP02836

MOLLE CAMERA MOUNT

This mount uses 2 adjacent loops across 2 rows of MOLLE webbing to hold your body-worn camera absolutely securely to your uniform.



WGP02614

SPARE CAMERA BATTERY

Extra shift? Overtime? No problem. Your body-worn camera has a detachable battery that can be changed in the field, giving virtually unlimited run-time. Take a spare battery wherever you go, so you're always ready for the unexpected.



Your officers need flexible solutions that can operate the way they do. The V300 continuous operation body-worn camera delivers ruggedness, endurance, and real-time integration with critical law enforcement technologies. Combined with streamlined device and evidence management software, it delivers clear video evidence to enhance safety, transparency and community trust. The V300 body-worn video solution is ready to go above and beyond the call of duty.

Learn more at www.motorolasolutions.com/v300

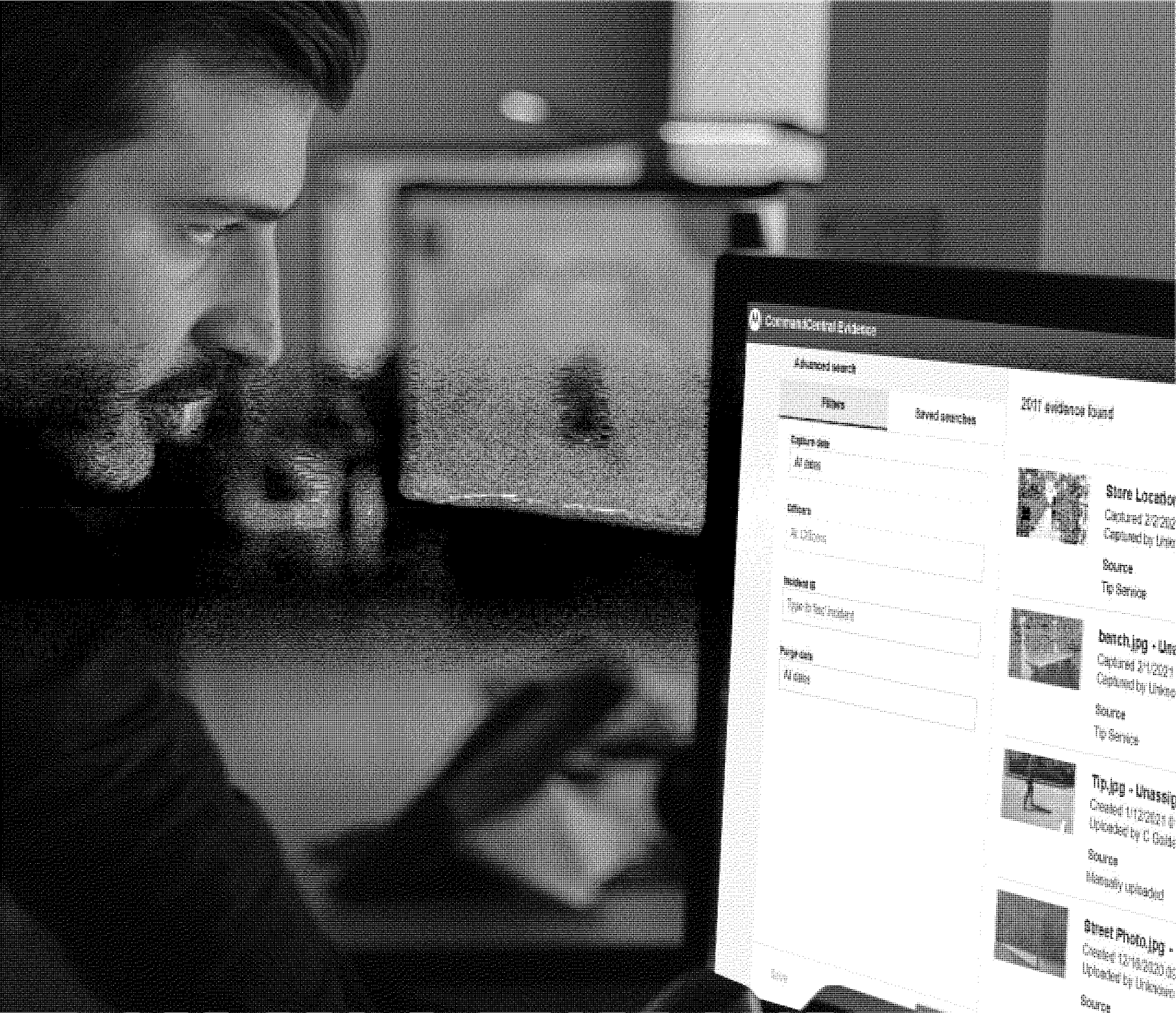


MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 300 West Monroe Street, Chicago, IL 60661 U.S.A. 888.361.2345 motorolasolutions.com

MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holding, LLC and are used under license. All other trademarks are the property of their respective owners. © 2021 Motorola Solutions, Inc. All rights reserved. 04/2021

ATF 2021-0948-RP6-000770



ENSURE JUSTICE IS ACHIEVED

**COMMANDCENTRAL EVIDENCE
DIGITAL EVIDENCE MANAGEMENT**





MAXIMIZE THE VALUE OF YOUR DIGITAL EVIDENCE

Digital Evidence can be one of the most valuable tools when investigating and prosecuting cases. But the extreme volume, variety and velocity of data has made digital evidence management more complex for public safety agencies than ever before. This creates barriers for law enforcement professionals when collecting, storing, securing, managing, and sharing this critical information.

You need to make sure your case isn't put at risk by missing valuable content. There are, in fact, instances where cases that don't include digital evidence may not be prosecuted at all — and missing digital evidence can result in a lawsuit.

It's time to revolutionize digital evidence management.

CommandCentral Evidence includes all the tools you need to collect evidence from citizens, capture media on scene, and centralize digital evidence storage. With cloud, hybrid and on-premises deployments available, knock down the data silos in your operations with the ability to manage, view and securely share the entire case from a single location.

ALL YOUR EVIDENCE IN ONE PLACE

SOURCE-AGNOSTIC DIGITAL EVIDENCE MANAGEMENT

With the influx of digital content, the last thing you need is to overwhelm your records and evidence teams with more to manage. CommandCentral Evidence minimizes the burden of new media by providing access to all case content from a single pane of glass, so you get the most out of your digital evidence. Whether it's fixed surveillance, body-worn camera video, in-car video, crime scene images, 9-1-1 audio or radio traffic, it all needs to be reviewed and potentially shared to aid in prosecution. Ingest or access content from any source via native integrations to our own portfolio, 3rd party system connectors or manual file uploading.

COMMUNITY INTERACTION TOOLS

Your community has valuable knowledge and can be a critical partner if you have the right tools to connect. Provide your citizens with the ability to share intelligence and be a true public safety partner with CommandCentral Community. These tools provide a secure way to collect evidence from the public, a safe place for anonymous tipping, and a channel to keep the public informed of local crime data — on your terms.

FIELD RESPONSE APPLICATION

Capture images, video and audio on scene with an Android or iOS mobile device. With CommandCentral Capture, all evidentiary data is isolated from personal data, making it inaccessible for tampering by other apps. The chain of custody is established at the moment of capture, so you never need to subpoena devices. The evidence is then automatically uploaded to CommandCentral Evidence for immediate use. Officers can also dictate their primary narrative directly from the app, saving valuable time with automated transcription.

IN-CAR AND BODY CAMERAS

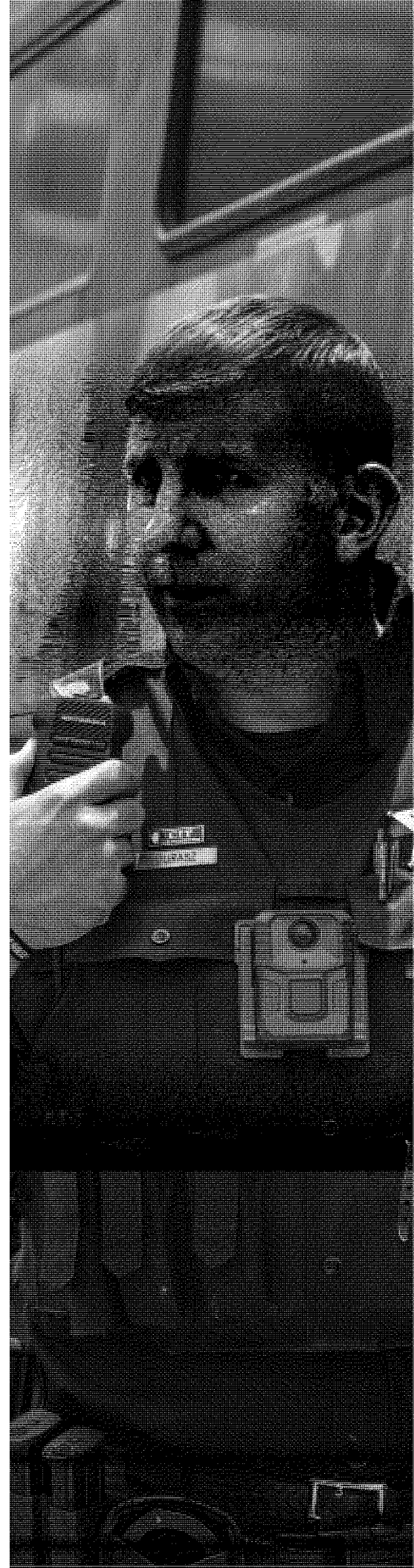
Capture secure, unbiased video evidence with Motorola Solutions' robust body-worn and in-car cameras. Driving out of the way to upload recorded video is expensive and unproductive. Keep patrol officers on the road with automatic, encrypted video uploads from in-car systems or WiFi-enabled body cameras directly to CommandCentral Evidence. Once the evidence is uploaded, synchronize playback so recorded video and audio from multiple devices can be seen and heard simultaneously.

MULTI-FILE ASSET UPLOAD

For multi-file evidence from physical media, the folder structure is just as important as the evidence itself. Maintain the integrity of the original evidence folder structure when you upload massive multi-file assets from physical media, such as DVDs, USBs and cellphones. This feature also saves on desktop storage, since it avoids uploading and downloading evidence as large zip files when needed for court. A security scan is run during the upload to protect against malware and other cyber threats.

THIRD PARTY CONNECTORS

Our public safety software suite is natively integrated with CommandCentral Evidence, making it easier to gather all of the content you need. But, even if you don't leverage our applications, we also have a third party connector ecosystem that allows you to interface with the investments you've already made and maximize the value of the digital content they produce. We've interfaced with many vendors across the public safety technology landscape already, and can work with you and your vendors to get one built if needed.



BUILD A STRONGER CASE

INTEGRATED RECORDS AND EVIDENCE MANAGEMENT

If you're like most agencies, siloed systems make it challenging to pull together a complete picture of a case in a timely manner for investigations. CommandCentral Evidence uses intelligent case folders that automatically aggregate all case data, so your detectives can focus on solving the crime. By leveraging agency-configurable tags, file metadata and correlation with your CAD and RMS, content is easier to search, manage and review. This saves time and resources that can be put to use on more value-added tasks.

COMMANDCENTRAL RECORDS

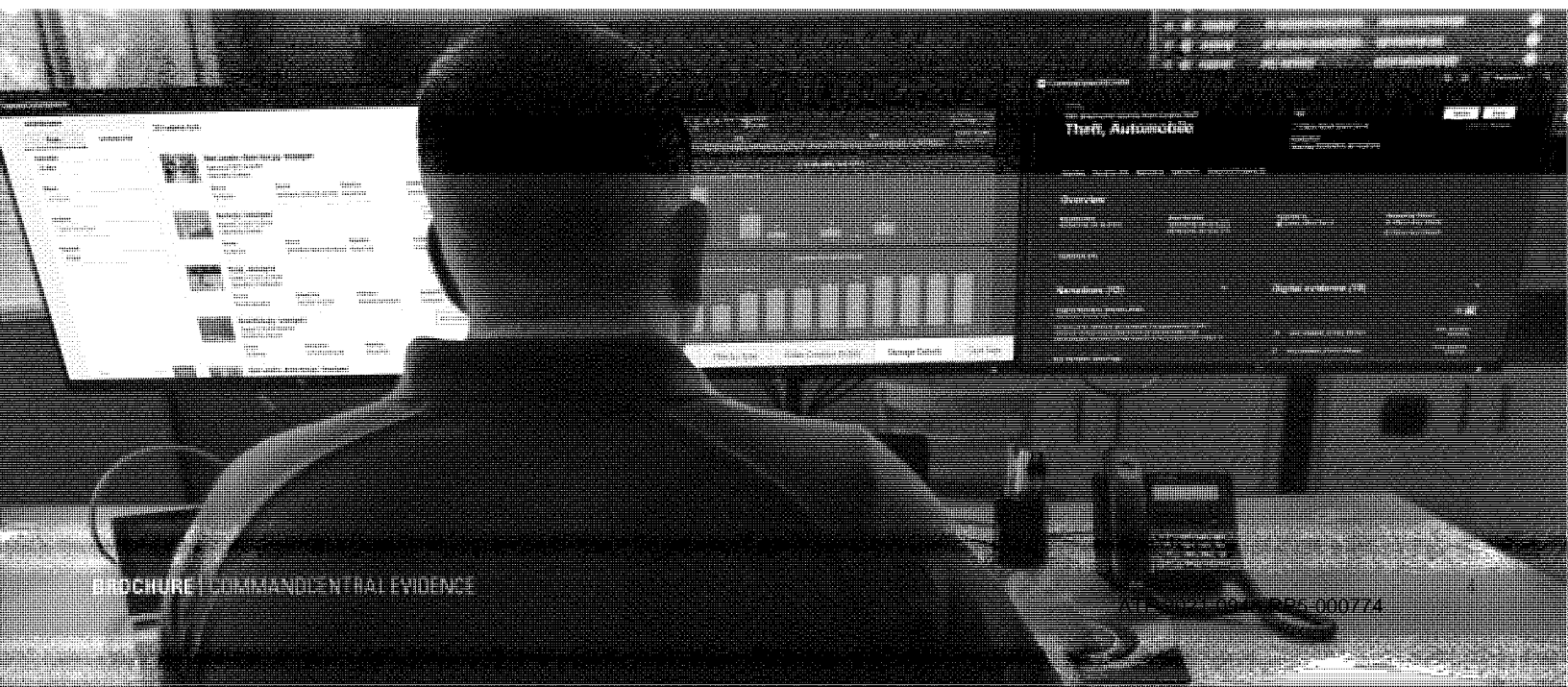
CommandCentral Evidence is completely integrated with CommandCentral Records, providing a more complete picture of the incident. The incident record automatically identifies links to existing person or vehicle records in the primary narrative, notifies you of license plate recognition database matches, and enables you to securely share the entire case from one location.

PREMIERONE AND SPILLMAN FLEX RECORDS

View digital evidence directly from your existing on-premises PremierOne Records or Spillman Flex Records system via an integrated module, making it easier to access and review all case-related information from one user interface.

THIRD PARTY CAD/RMS CORRELATION

Correlate digital evidence to your third party CAD/RMS system, taking content organization to another level. By leveraging metadata and applying tags to your content, you can automate the association of case-identifying details and minimize manual data input.



GO TO COURT WITH CONFIDENCE

SIMPLIFY JUDICIAL COLLABORATION

Successful prosecutions rely heavily on digital evidence. Collaboration with prosecutors, agency partners and the community must be seamless. Evidence must be shared in a timely manner and be fully tracked and audited. Perhaps most importantly, the chain of custody must be preserved. CommandCentral Evidence provides the tools to achieve the proper criminal outcomes and maintain transparency by securely sharing the case with the chain of custody intact.

JUDICIAL SHARING

Quick, easy and secure sharing of case information with partners is critical. Keep partners up-to-date by providing them with an account for in-app sharing or access to a dedicated, streamlined page for prosecutors. This allows them to access all of the case content shared with them — even from multiple agencies — from one, secure location.

AUDIT LOGGING

If content can't be authenticated and chain of custody kept unbroken, you risk your valuable evidence being dismissed. Detailed audit logging allows you to track all activity on or with a piece of content to ensure admissibility in court.

DOWNLOAD MANAGER

You may already have case sharing systems in place with your partners. Easily download content and audit logs to review and share. This allows you to leverage your agency's existing investments, while still enjoying the benefits of CommandCentral Evidence.

REDACTION SUITE

Freedom of information requests are a reality of the job, but it doesn't have to be inefficient. Our comprehensive redaction suite provides all the tools you need in one place to easily protect the privacy of those involved in an incident, while maintaining transparency to the public.



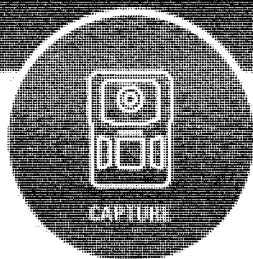
STREAMLINE YOUR DIGITAL EVIDENCE WORKFLOW

FROM CITIZEN TO COURTROOM

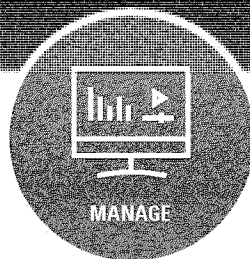
Knock down the data silos between your teams and tools with the confidence that every detail has been captured and no evidence left behind. From citizen to courtroom, intuitively collect, capture, manage and share all case content through one pane of glass that centralizes all evidence types for improved accuracy and collaboration.



COLLECT



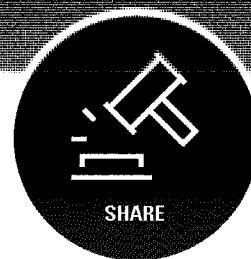
CAPTURE



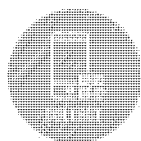
MANAGE



STREAMLINE



SHARE



COMMUNITY ENGAGEMENT

Collect anonymous tips and gather digital evidence directly from citizens via a simple form or agency generated link.



FIELD RESPONSE APPLICATION & VIDEO DEVICES

Capture images, video and audio on scene with a mobile device, in-car, or body camera.



DIGITAL EVIDENCE MANAGEMENT

Aggregate and intelligently organize all digital evidence from a variety of systems in one place.



RECORDS MANAGEMENT

Easily view all incident information within one, intelligently organized user interface, including the associated digital evidence.



JUDICIAL SHARING

Securely share with prosecutors, other agencies and the community with chain of custody intact.



TRANSFORM OPERATIONS WITH BIG DATA

You are faced with a ton of data — and it's only continuing to increase. It's structured and unstructured. It's coming in from so many different sources that it's easy to miss connections and trends. And no matter how much data you have, it won't be useful unless you can put it to work for your organization. Big data can be transformative to operations if it can be centralized and harnessed to fuel analytics.

UNIFIED SEARCH

You need to be able to find what you need, fast. Our free-text search makes it easier to find the content you're looking for amongst the sea of images, audio, video, and other files. You can even filter and group based on tags and any other metadata attributes. Save frequent searches so they dynamically update with any new content.

REPORTING

Dive deeper into your body camera program with built-in reports and dashboards. These reports provide insight into body camera usage and adoption, such as average video length and volume, policy compliance, officer behavioral changes and storage trends to help estimate future storage needs.

MACHINE LEARNING

Officers dictate their narrative from CommandCentral Capture. The transcript becomes the primary narrative in CommandCentral Records, and machine learning automatically links any existing person, vehicle, organization or location records.

SECURITY

Sensitive content may need to be restricted from certain users, or investigative groups might need to be alerted to review assets for particular cases. Simplify both of these processes by controlling who can access what with detailed permissions, and flagging or marking for-review content that requires special attention.

COMMANDCENTRAL

The industry's most integrated public safety software suite from call to case closure.

Incident Awareness

COMMUNITY
ENGAGEMENT



Citizen

EMERGENCY CALL
MANAGEMENT



911 Call Taker

VOICE &
COMPUTER
AIDED DISPATCH



Dispatcher

REAL-TIME
INTELLIGENCE
OPERATIONS



Intelligence
Analyst

FIELD RESPONSE
& REPORTING



Frontline
Responder

RECORDS
& EVIDENCE
MANAGEMENT



Records
Specialist

Post-Incident Resolution

ANALYSIS &
INVESTIGATION



Crime
Analyst

JAIL & INMATE
MANAGEMENT



Corrections
Officer

NEXT-GENERATION EVOLUTION WITH A DEDICATED TECHNOLOGY LEADER

We build software for mission-critical environments where every second matters. CommandCentral Evidence and other applications in our CommandCentral software suite unify data and streamline workflows from call to case closure in order to put your information to better use, improve safety for critical personnel and restore your focus on the communities you serve. Backed by a trusted, 90-year industry expert with proven public safety leadership, our suite is transforming the public safety experience with a focus on evolution, not revolution, in order to help you digitally transform your operation.

For more information about CommandCentral Evidence,
visit www.motorolasolutions.com/evidence



Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 U.S.A. motorolasolutions.com

MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. © 2021 Motorola Solutions, Inc. All rights reserved. 03-2021

ATF-2021-0948-RP5-000778

To: (b) (6), (b) (7)(C)
From: (b) (6), (b) (7)(C)
Sent: Tue 7/6/2021 3:10:59 PM
Subject: PIA Agent and TFO
ATF Axon Evidence PIA_07-06-2021 (b) (6), (b) (7)(C) updates.docx

Hi,

I made an attempt to edit the PIA so it applies to both ATF Special agents as well as TFO's. I also changed the contractor wording to allow ATF contractors to have access. I will let you use your expertise to incorporate the OST information (b) (6), (b) (7)(C) sent us.

I hope you enjoyed your holiday!

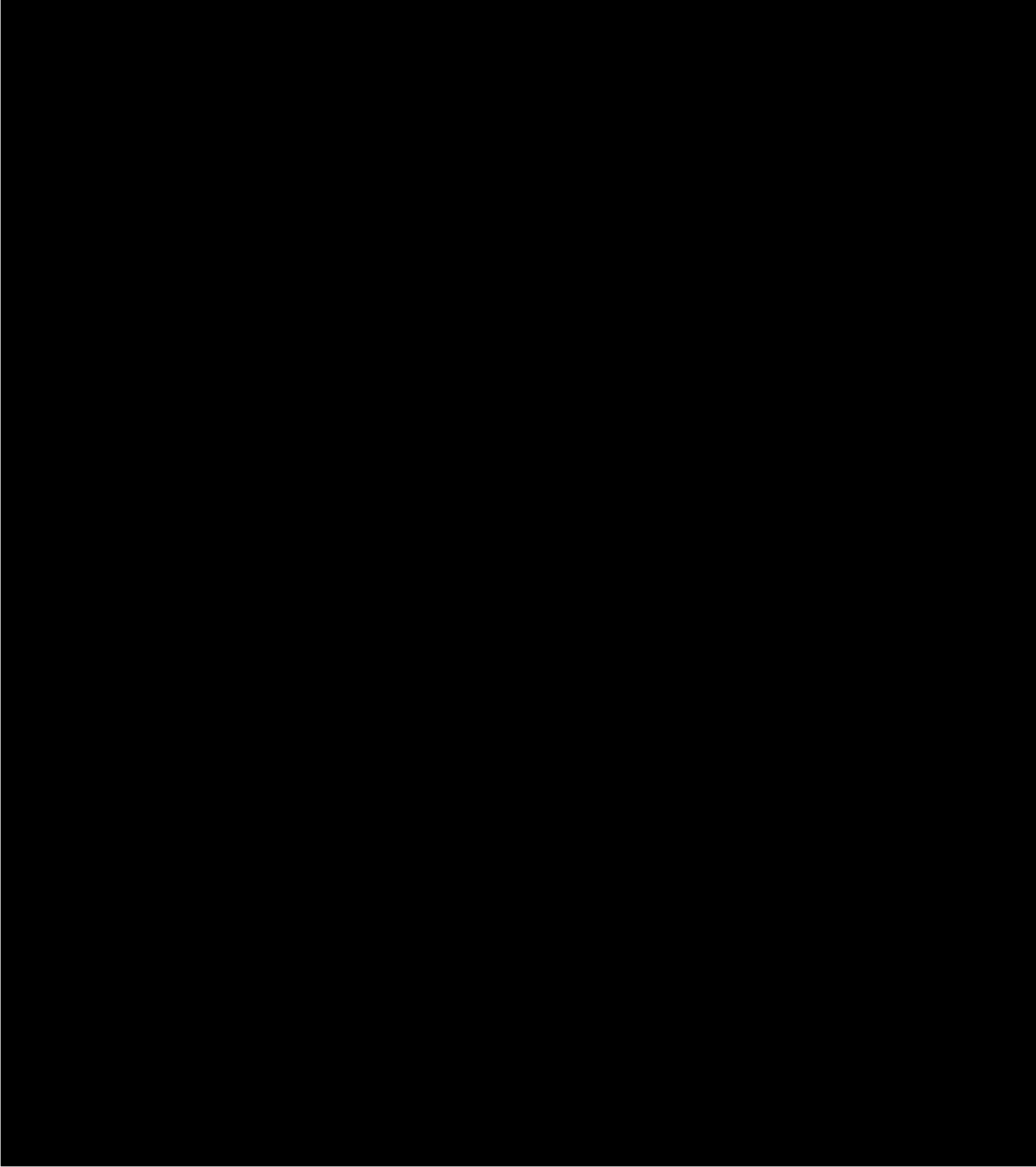
(b) (6), (b) (7)(C)

(b) (6), (b) (7)(C)
Alcohol, Tobacco, Firearms and Explosives
16009 N. 81st Street, Suite 100
Scottsdale, AZ 85260
Special Agent Project Officer-Digital Evidence Management
Technical Project Office
Special Operations Division
(b) (6), (b) (7)(C)

CONFIDENTIALITY NOTICE: E-mail may contain confidential information that is legally privileged. Do not read this e-mail if you are not the intended recipient.

This e-mail transmission, and any documents, files or previous e-mail messages attached to it may contain confidential information that is legally privileged. If you are not the intended recipient, or a person responsible for delivering it to the intended recipient, you are hereby notified that any disclosure, copying, distribution or use of any of the information contained in or attached to this transmission is **STRICTLY PROHIBITED**. If you have received this transmission in error, please immediately notify us by reply e-mail, by forwarding this to (b) (6), (b) (7)(C) or by telephone at (b) (6), (b) (7)(C) and destroy the original transmission and its attachments without reading or saving in any manner. Thank you.

(b) (5), (b) (6)



(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

To: (b) (6), (b) (7)(C)
Cc: (b) (6), (b) (7)(C)
From: (b) (6), (b) (7)(C)
Sent: Mon 7/12/2021 8:32:56 PM
Subject: BWC SRT Exemption

Good afternoon,

I am in the process of creating the Phase I BWC SOP. This will be a 6 month "trial" use of BWC's in the field, specifically the Detroit FD, Phoenix FD, and the ATF National Academy. (b) (5)

(b) (5)
Phase II will include a 12 month process of deploying BWC's to all the ATF field divisions.

(b) (5)

Thank you in advance for your help on this!

(b) (6), (b) (7)(C)
Alcohol, Tobacco, Firearms and Explosives
16009 N. 81st Street, Suite 100
Scottsdale, AZ 85260
Special Agent Project Officer-Digital Evidence Management
Technical Project Office
Special Operations Division
(b) (6), (b) (7)(C)

CONFIDENTIALITY NOTICE: E-mail may contain confidential information that is legally privileged. Do not read this e-mail if you are not the intended recipient.

This e-mail transmission, and any documents, files or previous e-mail messages attached to it may contain confidential information that is legally privileged. If you are not the intended recipient, or a person responsible for delivering it to the intended recipient, you are hereby notified that any disclosure, copying, distribution or use of any of the information contained in or attached to this transmission is STRICTLY PROHIBITED. If you have received this transmission in error, please immediately notify us by reply e-mail, by forwarding this to (b) (6), (b) (7)(C) or by telephone at (b) (6), (b) (7)(C) and destroy the original transmission and its attachments without reading or saving in any manner. Thank you.

To: (b) (6), (b) (7)(C)
From: (b) (6), (b) (7)(C)
Sent: Tue 7/20/2021 4:26:11 AM
Subject: RE: SRT Redaction Request: Body Worn Camera Update and Request for Information (Immediate Request for Assistance)

(b) (6), (b) (7)

The below information represents responses from SRT 2, SRT 3, SRT 5, SRT K9, SRT Training Manager & TMB TSS regarding redaction of ATF SRT's tactics, techniques & procedures (TTPs).

(b) (5)

(b) (5)

(b) (5)

Begin forwarded message:

From: (b) (6), (b) (7)(C)
Date: July 14, 2021 at 16:35:01 CDT
To: (b) (6), (b) (7)(C) >, (b) (6), (b) (7)(C) >, (b) (6), (b) (7)(C)
(b) (6), (b) (7)(C) (b) (6), (b) (7)(C) (b) (6), (b) (7)(C)
(b) (6), (b) (7)(C) (b) (6), (b) (7)(C)
(b) (6), (b) (7)(C) (b) (6), (b) (7)(C)
(b) (6), (b) (7)(C), (b) (6), (b) (7)(C) (b) (6), (b) (7)(C)
(b) (6), (b) (7)(C)
Cc: (b) (6), (b) (7)(C) "Vanderplow, Paul D"
(b) (6), (b) (7)(C) (b) (6), (b) (7)(C)
Subject: Body Worn Camera Update and Request for Information (Immediate Request for Assistance)

Gentlemen,

We have a deadline of Monday COB on this issue. Please forward all information to (b) (6), (b) (7)(C) so that he can organize and write SRT's position on Body Worn Cameras (BWCs).

Well, we all expected at some point that ATF's efforts to exempt SRT from BWCs would fail, but it failed earlier than anticipated. (b) (5)
(b) (5). In order to justify the redactions, we need to provide a justification and list of specific tactics, techniques, equipment, that should be redacted.

A few examples are below:

(b) (5)

Thanks.

(b) (6), (b) (7)(C)

Deputy Chief, SOD

Office: (b) (6), (b) (7)(C)

Cell: (b) (6), (b) (7)(C)

To: (b) (6), (b) (7)(C)
From: (b) (6)
Sent: Tue 6/29/2021 12:35:46 AM
Subject: Assistance body-worn camera accountability

Good evening,

As you may or may not be aware, per the Deputy Attorney General's directive, ATF is developing a body-worn camera program for ATF special agents. Phase one of the program implementation includes the deployment of hardware to include body-worn cameras (220) and the associated accessories. The initial deployment of cameras will be distributed to the following locations; Phoenix FD, Detroit FD and the ATF National Academy.

I am hoping for suggestions and guidance as to the most efficient way to pin these items. Cameras deployed to the Field Divisions will be assigned to the individual agents while the academy cameras will remain at the academy. The cameras will need to be pinned and assigned before the scheduled training in August.

Any suggestions or assistance would be appreciated.

(b) (6), (b) (7)(C)
Alcohol, Tobacco, Firearms and Explosives
16009 N. 81st Street, Suite 100
Scottsdale, AZ 85260
Special Agent Project Officer-Digital Evidence Management
Technical Project Office
Special Operations Division
(b) (6), (b) (7)(C)

CONFIDENTIALITY NOTICE: E-mail may contain confidential information that is legally privileged. Do not read this e-mail if you are not the intended recipient.

This e-mail transmission, and any documents, files or previous e-mail messages attached to it may contain confidential information that is legally privileged. If you are not the intended recipient, or a person responsible for delivering it to the intended recipient, you are hereby notified that any disclosure, copying, distribution or use of any of the information contained in or attached to this transmission is **STRICTLY PROHIBITED**. If you have received this transmission in error, please immediately notify us by reply e-mail, by forwarding this to (b) (6), (b) (7)(C) or by telephone at (b) (6), (b) (7)(C) and destroy the original transmission and its attachments without reading or saving in any manner. Thank you.

To: (b) (6), (b) (7)(C)
Cc: (b) (6), (b) (7)(C) SOD-SRT Team 2 Full Timers (b) (2) @atf.gov]
From: Redd, Robert K.
Sent: Thur 7/15/2021 10:05:36 PM
Subject: RE: Body Worn Camera Update and Request for Information (Immediate Request for Assistance)

(b) (6), (b) (7)(C)

Here is some additional input for the “redacted” list (FT dudes – thanks for the input).

Original List send from (b) (6), (b) (7)(C) with additions in Red:

(b) (5)

(b) (5)

Thanks-

(b) (6), (b) (7)(C)

(b) (6), (b) (7)(C)

ATF-Special Response Team 2

Cell (b) (6), (b) (7)(C)

(b) (6), (b) (7)(C)

From: (b) (6), (b) (7)(C)

Sent: Wednesday, July 14, 2021 5:35 PM

To: (b) (6), (b) (7)(C); (b) (6), (b) (7)(C); (b) (6), (b) (7)(C) (Dallas)

(b) (6), (b) (7)(C); (b) (6), (b) (7)(C); (b) (6), (b) (7)(C)

(b) (6), (b) (7)(C); (b) (6), (b) (7)(C); (b) (6), (b) (7)(C)

(b) (6), (b) (7)(C); (b) (6), (b) (7)(C); (b) (6), (b) (7)(C)

(b) (6), (b) (7)(C); (b) (6), (b) (7)(C)

Cc: (b) (6), (b) (7)(C); Vanderplow, Paul D; (b) (6), (b) (7)(C)

(b) (6), (b) (7)(C)

Subject: Body Worn Camera Update and Request for Information (Immediate Request for Assistance)

Importance: High

Gentlemen,

We have a deadline of Monday COB on this issue. Please forward all information to (b) (6), (b) (7)(C) so that he can organize and write SRT's position on Body Worn Cameras (BWCs).

Well, we all expected at some point that ATF's efforts to exempt SRT from BWCs would fail, but it failed earlier than anticipated. (b) (5)

(b) (5) In order to justify the redactions, we need to provide a justification and list of specific tactics, techniques, equipment, that should be redacted.

A few examples are below:

(b) (5)

(b) (5)

Thanks.

(b) (6), (b) (7)(C)

Deputy Chief, SOD

Office: (b) (6), (b) (7)(C)

Cell: (b) (6), (b) (7)(C)

To: (b) (6), (b) (7)(C)
From: (b) (6), (b) (7)(C)
Sent: Fri 7/16/2021 8:16:45 PM
Subject: PIA Approval

Ma'am,

We are hoping to start Phase I of the BWC program on September 1, 2021, what is our timeline for approval of the PIA?

(b) (6), (b) (7)(C)
Alcohol, Tobacco, Firearms and Explosives
16009 N. 81st Street, Suite 100
Scottsdale, AZ 85260
Special Agent Project Officer-Digital Evidence Management
Technical Project Office
Special Operations Division
(b) (6), (b) (7)(C)

CONFIDENTIALITY NOTICE: E-mail may contain confidential information that is legally privileged. Do not read this e-mail if you are not the intended recipient.

This e-mail transmission, and any documents, files or previous e-mail messages attached to it may contain confidential information that is legally privileged. If you are not the intended recipient, or a person responsible for delivering it to the intended recipient, you are hereby notified that any disclosure, copying, distribution or use of any of the information contained in or attached to this transmission is **STRICTLY PROHIBITED**. If you have received this transmission in error, please immediately notify us by reply e-mail, by forwarding this to (b) (6), (b) (7)(C) or by telephone at (b) (6), (b) (7)(C) and destroy the original transmission and its attachments without reading or saving in any manner. Thank you.

To: (b) (6), (b) (7)(C)
From: (b) (6), (b) (7)(C)
Sent: Fri 7/16/2021 8:19:07 PM
Subject: RE: PIA Approval

The PIA is with (b) (6), (b) (7)(C) for the ISSM review and will be returned back to OPCL – it was changed (after the 1st OPCL) review to account for the change in policy.

From: (b) (6), (b) (7)(C)
Sent: Friday, July 16, 2021 4:17 PM
To: (b) (6), (b) (7)(C)
Subject: PIA Approval

Ma'am,

We are hoping to start Phase I of the BWC program on September 1, 2021, what is our timeline for approval of the PIA?

(b) (6), (b) (7)(C)
Alcohol, Tobacco, Firearms and Explosives
16009 N. 81st Street, Suite 100
Scottsdale, AZ 85260
Special Agent Project Officer-Digital Evidence Management
Technical Project Office
Special Operations Division
(b) (6), (b) (7)(C)

CONFIDENTIALITY NOTICE: E-mail may contain confidential information that is legally privileged. Do not read this e-mail if you are not the intended recipient.

This e-mail transmission, and any documents, files or previous e-mail messages attached to it may contain confidential information that is legally privileged. If you are not the intended recipient, or a person responsible for delivering it to the intended recipient, you are hereby notified that any disclosure, copying, distribution or use of any of the information contained in or attached to this transmission is **STRICTLY PROHIBITED**. If you have received this transmission in error, please immediately notify us by reply e-mail, by forwarding this to (b) (6), (b) (7)(C) or by telephone at (b) (6), (b) (7)(C) and destroy the original transmission and its attachments without reading or saving in any manner. Thank you.

To: (b) (6), (b) (7)(C)
From: (b) (6), (b) (7)(C)
Sent: Tue 7/20/2021 8:50:06 PM
Subject: Final 1851.7 for Body-Worn Camera hardware
Receiving Report 1851.7 Flex 2 Camera 1-19-signed.pdf
Receiving Report 1851.7 Flex 2 Camera 20-30 signed.pdf

(b) (6), (b) (7)(C),

These are the final two 1851.7's for the body-worn camera hardware we received.

These are the Flex 2 cameras that attach to the previously submitted Flex 2 Controllers.

I also noticed a mistake in the previous submission of the Flex two controllers. The price for the controllers is (b) (4) per controller. The price of the Flex 2 Cameras are (b) (4) per camera. Please let me know if you would like me to resubmit the 1851.7 for the controllers or if you can change it on your end. I apologize for the mistake.

(b) (6), (b) (7)

(b) (6), (b) (7)(C)
Alcohol, Tobacco, Firearms and Explosives
16009 N. 81st Street, Suite 100
Scottsdale, AZ 85260
Special Agent Project Officer-Digital Evidence Management
Technical Project Office
Special Operations Division
(b) (6), (b) (7)(C)

CONFIDENTIALITY NOTICE: E-mail may contain confidential information that is legally privileged. Do not read this e-mail if you are not the intended recipient.

This e-mail transmission, and any documents, files or previous e-mail messages attached to it may contain confidential information that is legally privileged. If you are not the intended recipient, or a person responsible for delivering it to the intended recipient, you are hereby notified that any disclosure, copying, distribution or use of any of the information contained in or attached to this transmission is **STRICTLY PROHIBITED**. If you have received this transmission in error, please immediately notify us by reply e-mail, by forwarding this to (b) (6), (b) (7)(C) or by telephone at (b) (6), (b) (7)(C) and destroy the original transmission and its attachments without reading or saving in any manner. Thank you.

FILE REMOVED:

PASSWORD PROTECTED

1-2

FILE REMOVED:

PASSWORD PROTECTED

2-2

To: (b) (6), (b) (7)(C) (b) (6), (b) (7)(C)
From: (b) (6), (b) (7)(C)
Sent: Mon 6/28/2021 7:11:42 PM
Subject: Simplified Diagram and Narrative
[Axon Encryption Description.docx](#)
[Visio-JCOTS Simplified Diagram.pdf](#)

(b) (6), (b) (7)(C) and (b) (6), (b) (7)(C)

I tried to put two things together to assist with the PIA. Let me know what else that you need. I can discuss and answer any questions tomorrow.

(b) (6), (b) (7)(C)

Operations Officer

Office of Science and Technology | Bureau of Alcohol, Tobacco, Firearms, & Explosives
7S-255 | 99 New York Ave, NE | Washington D.C. 20226

Mobile: (b) (6), (b) (7)(C)

Email: (b) (6), (b) (7)(C)



Security for the ATF BWC Camera Program

Authentication:

All Agents and TFO's that will access the Axon evidence.com system must access from an ATF physical or virtual (remote access VPN) network. They will use their PIV card and sign into the ATF evidence.com services after having authenticated to the ATF Active Directory through their ATF ESA laptop.

Agents and TFO's will request access to the ATF BWC program through the Special Operations Division and its program office. Agents and TFO's will only be granted access to their case data or associated records and evidence.

Network Protections:

Access to ATF's evidence.com services must traverse the Department's Justice Cloud Optimized TIC Services (JCOTS) program. The JCOTS program provides several layers of network and application protection. These protections include forward proxies that log all activity associated with a connection the service. Also, the Department does have data loss prevention services that restricts the flow of PII from ATF and other components to external services. This includes breaking the encryption of traffic leaving the Department and re-encrypting after completing analysis.

Encryption:

All transmissions from users and Axon docks connect to Axon using TLS 1.2 encryption using a 256-bit key and perfect forward that changes keys frequently to reduce any possible data loss. This is fully encrypted throughout transmission. Also, this traffic does traverse Departmental Wide Area Network (WAN) that is also encrypted using FIPS 140-2 encryption algorithms.

All data that resides within evidence.com is stored with CJIS compliant NSA Suite B 256-bit AES encryption.

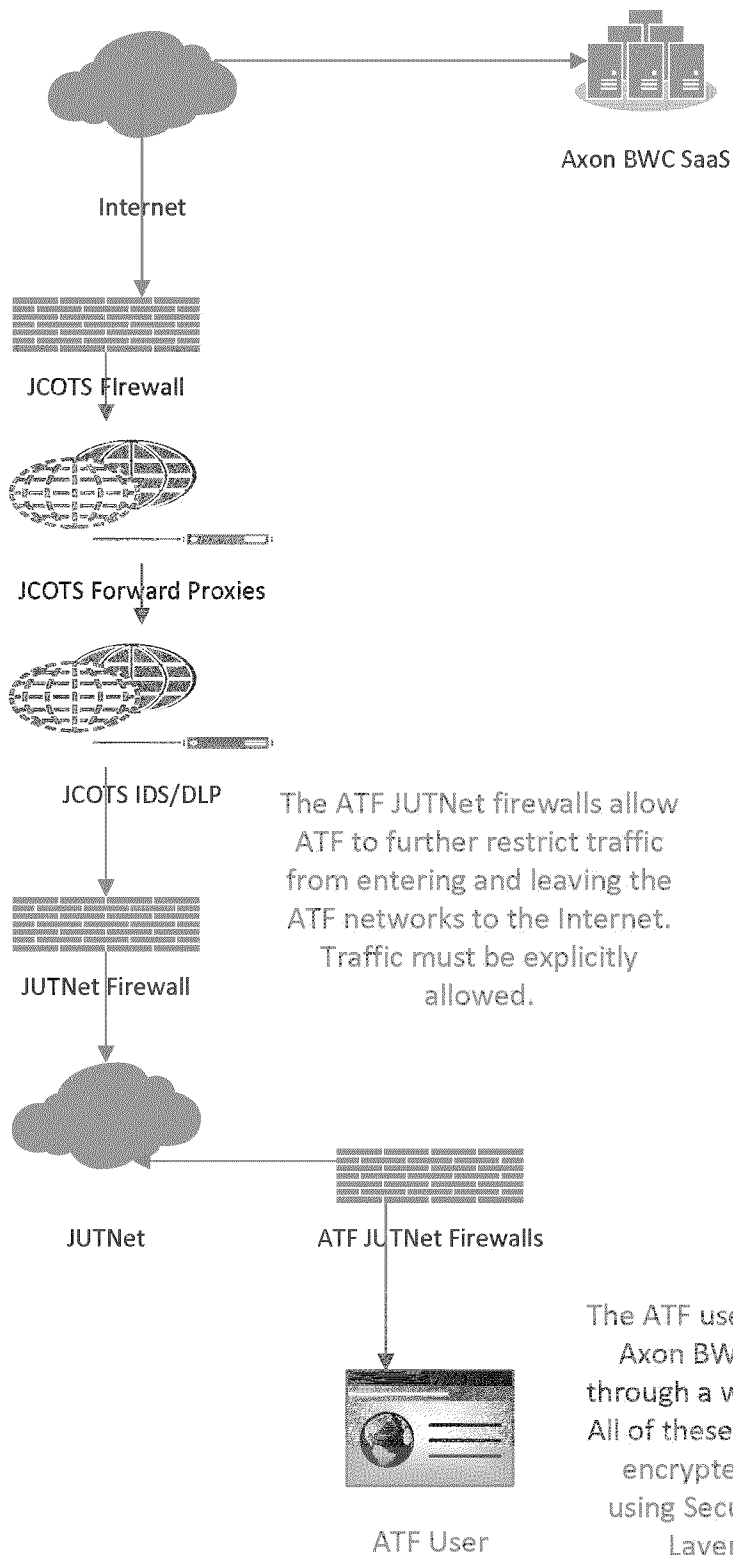
Any data that is downloaded from evidence.com will be stored on an ATF laptop that is encrypted with Microsoft Bitlocker encryption. Also, any data that is stored on the network will be stored in the Department's and ATF's Office365 system on OneDrive that is also encrypted using 256-bit keys.

The JUTNet firewalls further restrict traffic from the Internet accessing internal Departmental networks. Traffic must be explicitly allowed.

The JCOTS IDS and data loss prevention system restrict types of data that may be sent to the Internet from internal networks to the Internet. For example: Social Security Numbers are flagged and denied.

The JUTNet firewalls further restrict traffic from the Internet accessing internal Departmental networks. Traffic must be explicitly allowed.

Overview: All traffic from an ATF office to the Internet is encrypted from the workstation until it gets to the Internet on the JUTNet network. JMD may decrypt the traffic to analyze for nefarious activity.



The ATF JUTNet firewalls allow ATF to further restrict traffic from entering and leaving the ATF networks to the Internet. Traffic must be explicitly allowed.

The ATF user will access Axon BWC services through a web browser. All of these sessions are encrypted to Axon using Secure Sockets Layer (SSL).

Cc: (b) (6), (b) (7)(C); (b) (6), (b) (7)(C)
To: (b) (6), (b) (7)(C)
From: (b) (6), (b) (7)(C)
Sent: Wed 8/11/2021 4:52:30 PM
Subject: Fwd: PIA - Axon Evidence
ATF Axon Evidence_PIA_08-10-2021.docx

Good to go

Begin forwarded message:

From: (b) (6), (b) (7)(C)
Date: August 10, 2021 at 8:51:12 PM EDT
To: (b) (6), (b) (7)(C)
Cc: (b) (6), (b) (7)(C); (b) (6), (b) (7)(C)
Subject: PIA - Axon Evidence

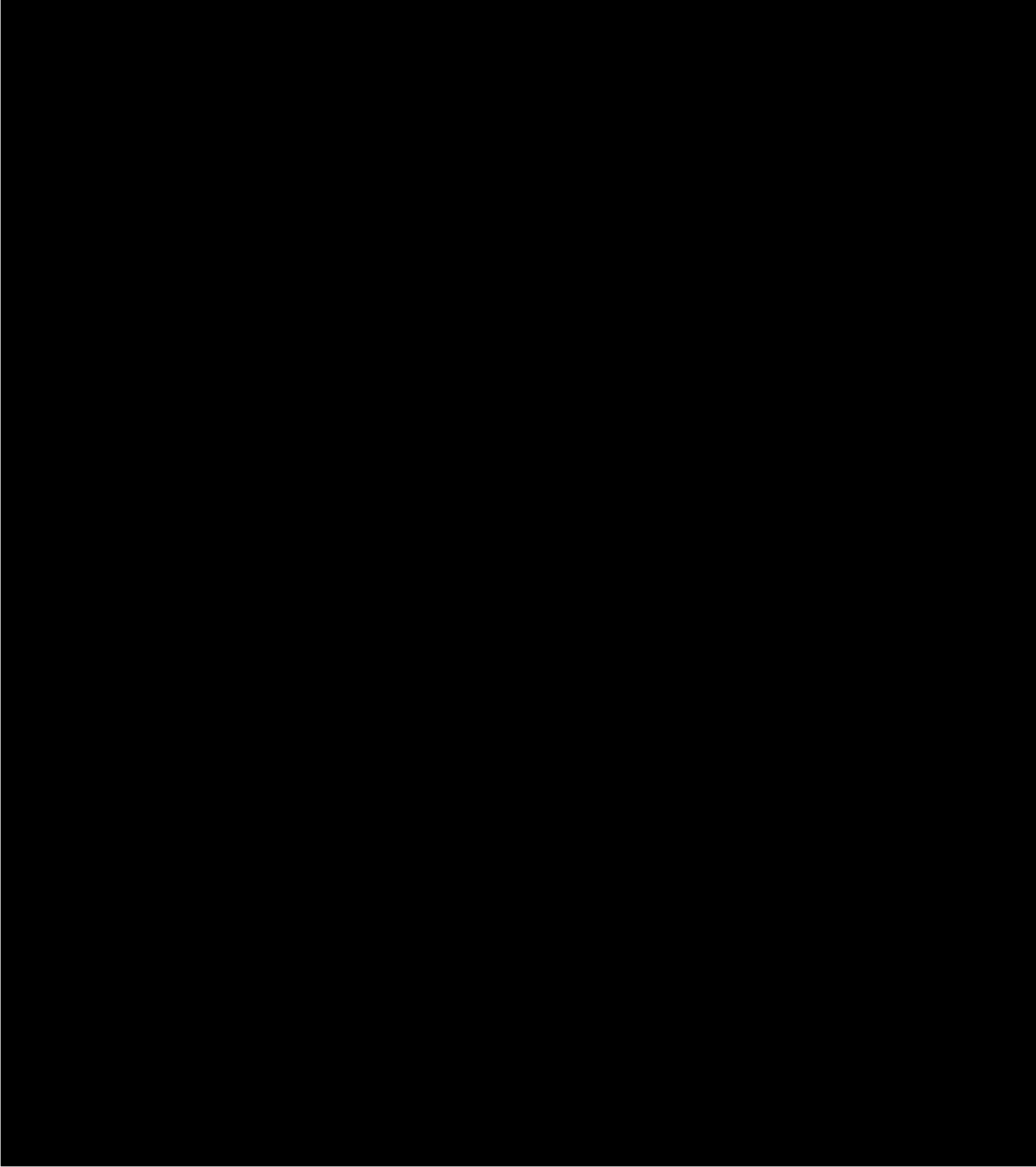
The attached is a re-write of the PIA for Axon – OPCL has made some changes to how they want the information described.

This is a good example of what they want to see now
(<https://www.justice.gov/opcl/page/file/1412716/download>).

V (b) (6), (b) (7)(C)

(b) (5)

(b) (5), (b) (6)



(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

To: (b) (6), (b) (7)(C)
Cc: TFO Management-JLEO Program[(b) (2) @atf.gov]; (b) (6), (b) (7)(C)
(Contractor)(b) (6), (b) (7)(C)
From: (b) (6), (b) (7)(C)
Sent: Tue 6/29/2021 2:56:06 PM
Subject: FW: (b) (6), (b) (7)(C) - Part I (Atlanta Field Division)

(b) (6), (b) (7)(C)

Please see below regarding an addendum for Atlanta FD.

Thanks!

(b) (6), (b) (7)(C)

(b) (6), (b) (7)(C)
Program Manager
Resource Management Branch - JLEO
(b) (6), (b) (7)(C) (cell)

From: TFO Management-JLEO Program (b) (2) @atf.gov>
Sent: Tuesday, June 29, 2021 9:54 AM
To: (b) (6), (b) (7)(C)
Cc: (b) (6), (b) (7)(C) (Contractor) (b) (6), (b) (7)(C)
Subject: FW: (b) (6), (b) (7)(C) - Part I (Atlanta Field Division)

Good Morning,

Do we have a copy of an addendum to send out?

Thanks,

(b) (6), (b) (7)(C)
Records Examiner Analyst
Resource Management Branch, JLEO
O: (b) (6), (b) (7)(C)

From: (b) (6), (b) (7)(C)
Sent: Tuesday, June 29, 2021 10:51 AM
To: TFO Management-JLEO Program (b) (2) @atf.gov>
Subject: FW: (b) (6), (b) (7)(C) - Part I (Atlanta Field Division)

Good Morning (b) (6), (b) (7)(C)

Do you have a copy of the addendum for the body worn camera that needs to be completed?

I sent an e-mail to the e-mail address (b) (2) @atf.gov and never got a response back.

Your assistance is appreciated.

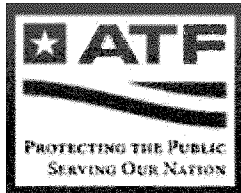
Thanks,

(b) (6), (b) (7)(C)

Senior Operations Officer
Senior Industry Operations Investigator
Bureau of Alcohol, Tobacco, Firearms & Explosives
Atlanta Field Division

(b) (6), (b) (7)(C) (office)

(b) (6), (b) (7)(C) (cell)



From: TFO Management-JLEO Program (b) (2) @atf.gov>
Sent: Tuesday, June 29, 2021 10:20 AM
To: (b) (6), (b) (7)(C) >; TFO Management-JLEO Program (b) (2) @atf.gov>
Subject: RE: (b) (6), (b) (7)(C) - Part I (Atlanta Field Division)

Good Morning,

Please provide the addendum for the body worn camera. Once received, we will continue with processing the security package.

Regards,

(b) (6), (b) (7)(C)

Records Examiner Analyst
Resource Management Branch, JLEO
O: (b) (6), (b) (7)(C)

From: (b) (6), (b) (7)(C)
Sent: Thursday, June 17, 2021 3:06 PM
To: TFO Management-JLEO Program (b) (2) @atf.gov>
Subject: (b) (6), (b) (7)(C) - Part I (Atlanta Field Division)

Good Afternoon -

See attached Part I documents, MOU and Photo for Macon Field Office, Atlanta Field Division TFO Candidate (b) (6), (b) (7)(C).

Thanks,

(b) (6), (b) (7)(C)

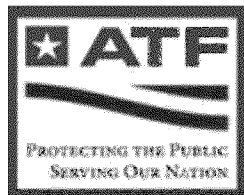
Senior Operations Officer
Senior Industry Operations Investigator

Bureau of Alcohol, Tobacco, Firearms & Explosives

Atlanta Field Division

(b) (6), (b) (7)(C) (office)

(b) (6), (b) (7)(C) (cell)



To: (b) (6), (b) (7)(C)
From: (b) (6), (b) (7)(C)
Sent: Wed 7/7/2021 7:28:21 PM
Subject: Guidance

Good Afternoon,

I'm reaching out in an effort to get some guidance reference our Body Worn Camera policy. One of our local law enforcement partner agencies (Anne Arundel County, MD Police Department) has started their BWC program and there is slight disagreement/difference in agency policy (ATF's & Anne Arundel County PD) with regards to retaining of digital evidence and releasing of digital evidence. Can you please provide step by step instructions on what we need to do with AA County TFO's and their BWC footage (just in case we have an operation/incident in which our ATF TFOs from AACo PD respond to an ATF lead investigation) since they are starting to use the BWCs?

Thanks in Advance,

(b) (6), (b) (7)(C)
Assistant Special Agent in Charge
Baltimore Field Division
31 Hopkins Plaza., 5th Floor
Baltimore, MD 21201
(b) (6), (b) (7)(C) (office)
(b) (6), (b) (7)(C) (cell)

To: (b) (6), (b) (7)(C)
From: (b) (6), (b) (7)(C)
Sent: Thur 9/2/2021 3:22:01 PM
Subject: MOUs
MOU JLEO TEMPLATE- MARCH 2021 - Revised 3.22.2021-Charlotte FD.docx

Good morning, (b) (6), (b) (7)(C)

Hope you've been well. I just wanted to clarify the BWC addendum/checklist policy since we are having many departments update their MOUs, which includes BWC language. (see attached). Our division counsel advised that whoever signs the new MOU does not to sign an addendum. The BWC addendum was only for departments that had the old MOU that was not up for renewal.

I had a few TFOs that checked their departments require BWC on planned federal operations and JLEO requested the addendum/checklist (new departments).

I just want to make sure I'm on the same page as everyone. Thanks in advance!

(b) (6), (b) (7)(C)
Senior Operations Officer
ATF Senior Special Agent

Charlotte Field Division
Bureau of Alcohol, Tobacco, Firearms & Explosives
3600 Arco Corporate Drive, Suite 500
Charlotte, NC 28273
Main: (b) (6), (b) (7)(C)
Fax: (b) (6), (b) (7)(C)
Cell: (b) (6), (b) (7)(C)

MEMORANDUM OF UNDERSTANDING

BETWEEN

THE BUREAU OF ALCOHOL, TOBACCO, FIREARMS AND EXPLOSIVES (ATF),

And

XXXXXXXXXX

This Memorandum of Understanding (“MOU”) is entered into by and between the Bureau of Alcohol, Tobacco, Firearms and Explosives (“ATF”) and _____ (“participating agency”) as it relates to the _____ Task Force (herein referred to as the “Task force”).

- *The MOU is specific to the task force being referenced and applies only to the above-named participating agency, although other agencies may also be taking part on the same task force.*

BACKGROUND

- *This section is optional.*

AUTHORITIES

The authority to investigate and enforce offenses under provisions of this MOU are found at 28 U.S.C. § 599A , 28 C.F.R. §§ 0.130, 0.131, and 18 U.S.C. § 3051.

PURPOSE

The Task Force will perform the activities and duties described below:

- a. Investigate firearms trafficking
 - b. Investigate firearms related violent crime
 - c. Gather and report intelligence data relating to trafficking in firearms
 - d. Conduct undercover operations where appropriate and engage in other traditional methods of investigation in order that the Task Force's activities will result in effective prosecution before the courts of the United States and the State of _____.
- *This section will vary depending upon the mission of the task force.*

MEASUREMENT OF SUCCESS

The success of this initiative will be measured by the participating agencies willingness to share certain information, (i.e crime statistics) for the purpose of measuring the success of the task force as well as its performance.

- *This section will vary depending upon Mission Activities Strategic Goals listed on page 6 of the FY 2017 – FY 2022 Strategic Plan. The ATF Performance Measurement Index is found on page 20, and the same performance indicators will be used. A copy of the plan can be found on the Strategic Management tab of the ATF Portal.*

PHYSICAL LOCATION

Officers/troopers/agents assigned to this Task Force by their employer shall be referred to as task force officers (TFOs). TFOs will be assigned to the ATF _____ Field Office and will be located at _____.

SUPERVISION AND CONTROL

The day-to-day supervision and administrative control of TFOs will be the mutual responsibility of the participants, with the ATF Special Agent in Charge or his/her designee having operational control over all operations related to this Task Force.

Each TFO shall remain subject to their respective agencies' policies, and shall report to their respective agencies regarding matters unrelated to this agreement/task force. With regard to matters related to the Task Force, TFOs will be subject to Federal law and Department of Justice (DOJ) and ATF orders, regulations and policy, including those related to standards of conduct, sexual harassment, equal opportunity issues and Federal disclosure laws.

Failure to comply with this paragraph could result in a TFO's dismissal from the Task Force.

- *This language does not dictate any particular command structure for TFs. As long as ATF retains supervisory authority, the internal organization of the TF is based on the discretion of ATF management. Therefore, this paragraph can be modified to incorporate state or local supervisory personnel into the command structure of the TF with the approval of FMS and Chief Counsel's Office.*

PERSONNEL, RESOURCES AND SUPERVISION

To accomplish the objectives of the Task Force, ATF will assign ___ Special Agents to the Task Force. ATF will also, subject to the availability of funds, provide necessary funds and equipment to support the activities of the ATF Special Agents and officers assigned to the Task Force. This support may include: office space, office supplies, travel funds, funds for the purchase of evidence and information, investigative equipment, training, and other support items.

- *This section will vary depending upon the resources ATF will commit to the task force.*

Each participating agency agrees to make available to their assigned task members any equipment ordinarily assigned for use by that agency. In the event ATF supplies equipment (which may include vehicles, weapons or radios), TFOs must abide by any applicable ATF property orders or policy, and may be required to enter into a separate agreement for their use.

To accomplish the objectives of the Task Force, the _____ agrees to detail _____ fulltime TFOs and/or _____ part time TFOs to the Task Force for a period of not less than two (2) years.

All TFOs shall qualify with their respective firearms by complying with ATF's Firearms and Weapons Policy.

SECURITY CLEARANCES

All TFOs will undergo a security clearance and background investigation, and ATF shall bear the costs associated with those investigations. TFOs must not be the subject of any ongoing investigation by their department or any other law enforcement agency, and past behavior or punishment, disciplinary, punitive or otherwise, may disqualify one from eligibility to join the Task Force. ATF has final authority as to the suitability of TFOs for inclusion on the Task Force.

DEPUTATIONS

ATF, as the sponsoring Federal law enforcement agency, may request at its sole discretion that the participating agency's TFOs be deputized by the U.S. Marshals Service to extend their jurisdiction, to include applying for and executing Federal search and arrest warrants, and requesting and executing Federal grand jury subpoenas for records and evidence involving violations of Federal laws. Such requests will be made on an individual basis as determined by ATF.

A TFO will not be granted Department of Justice legal representation if named as a defendant in a private-capacity lawsuit alleging constitutional violations unless all deputation paperwork has been completed prior to the event(s) at issue in the lawsuit.

The participating agencies agree that any Federal authority that may be conferred by a deputation is limited to activities supervised by ATF and will terminate when this MOU is terminated or when the deputized TFOs leave the Task Force, or at the discretion of ATF.

ASSIGNMENTS, REPORTS AND INFORMATION SHARING

An ATF supervisor or designee will be empowered with designated oversight for investigative and personnel matters related to the Task Force and will be responsible for opening, monitoring, directing and closing Task Force investigations in accordance with ATF policy and the applicable United States Attorney General's Guidelines.

Assignments will be based on, but not limited to, experience, training and performance, in addition to the discretion of the ATF supervisor.

All investigative reports will be prepared utilizing ATF's investigative case management system, (N-Force) utilizing ATF case report numbers. The participating agency will share investigative reports, findings, intelligence, etc., in furtherance of the mission of this agreement, to the fullest extent allowed by

law. For the purposes of uniformity, there will be no duplication of reports, but rather a single report prepared by a designated individual which can be duplicated as necessary. Every effort should be made to document investigative activity on ATF Reports of Investigation (ROI), unless otherwise agreed to by ATF and the participating agency(ies). This section does not preclude the necessity of individual TFOs to complete forms required by their employing agency.

Information will be freely shared among the TFOs and ATF personnel with the understanding that all investigative information will be kept strictly confidential and will only be used in furtherance of criminal investigations. No information gathered during the course of the Task Force, to include informal communications between TFOs and ATF personnel, may be disseminated to any third party, non-task force member by any task force member without the express permission of the ATF Special Agent in Charge or his/her designee.

Any public requests for access to the records or any disclosures of information obtained by task force members during Task Force investigations will be handled in accordance with applicable statutes, regulations, and policies pursuant to the Freedom of Information Act and the Privacy Act and other applicable federal and/or state statutes and regulations.

INVESTIGATIVE METHODS

The parties agree to utilize Federal standards pertaining to evidence handling and electronic surveillance activities to the greatest extent possible. However, in situations where state or local laws are more restrictive than comparable Federal law, investigative methods employed by state and local law enforcement agencies shall conform to those requirements, pending a decision as to a venue for prosecution.

The use of other investigative methods (search warrants, interceptions of oral communications, etc.) and reporting procedures in connection therewith will be consistent with the policy and procedures of ATF. All Task Force operations will be conducted and reviewed in accordance with applicable ATF and Department of Justice policy and guidelines.

None of the parties to this MOU will knowingly seek investigations under this MOU that would cause a conflict with any ongoing investigation of an agency not party to this MOU. It is incumbent upon each participating agency to notify its personnel regarding the Task Force's areas of concern and jurisdiction. All law enforcement actions will be coordinated and cooperatively carried out by all parties to this MOU.

INFORMANTS

ATF guidelines and policy regarding the operation of informants and cooperating witnesses will apply to all informants and cooperating witnesses directed by TFOs.

Informants developed by TFOs may be registered as informants of their respective agencies for administrative purposes and handling. The policies and procedures of the participating agency with regard to handling informants will apply to all informants that the participating agency registers. In addition, it will be incumbent upon the registering participating agency to maintain a file with respect to the performance of all informants or witnesses it registers. All information obtained from an informant

and relevant to matters within the jurisdiction of this MOU will be shared with all parties to this MOU. The registering agency will pay all reasonable and necessary informant expenses for each informant that a participating agency registers.

DECONFLICTION

Each participating agency agrees that the deconfliction process requires the sharing of certain operational information with the Task Force, which, if disclosed to unauthorized persons, could endanger law enforcement personnel and the public. As a result of this concern, each participating agency agrees to adopt security measures set forth herein:

- a. Each participating agency will assign primary and secondary points of contact.
- b. Each participating agency agrees to keep its points of contact list updated.

The points of contact for this Task Force are:

ATF: _____

Participating Agency: _____

EVIDENCE

Evidence will be maintained by the lead agency having jurisdiction in the court system intended for prosecution. Evidence generated from investigations initiated by a TFO or ATF special agent intended for Federal prosecution will be placed in the ATF designated vault, using the procedures found in ATF orders.

All firearms seized by a TFO must be submitted for fingerprint analysis and for a National Integrated Ballistic Information Network (NIBIN) examination. Once all analyses are completed, all firearms seized under Federal law shall be placed into the ATF designated vault for proper storage. All firearms information/descriptions taken into ATF custody must be submitted to ATF's National Tracing Center.

- *This could be modified to include DNA testing of all firearms taken into custody by the task force.*

JURISDICTION/PROSECUTIONS

Cases will be reviewed by the ATF Special Agent in Charge or his/her designee in consultation with the participating agency and the United States Attorney's Office and appropriate State's attorney offices, to determine whether cases will be referred for prosecution to the U.S. Attorney's Office or to the relevant State's attorney's office. This determination will be based upon which level of prosecution will best serve the interests of justice and the greatest overall benefit to the public. Any question that arises pertaining to prosecution will be resolved through discussion among the investigative agencies and prosecuting entities having an interest in the matter.

In the event that a state or local matter is developed that is outside the jurisdiction of ATF or it is decided that a case will be prosecuted on the state or local level, ATF will provide all relevant information to state and local authorities, subject to Federal law. Whether to continue investigation of state and local crimes is at the sole discretion of the state or local participating agency.

USE OF FORCE

All fulltime TFOs will comply with ATF and the Department of Justice's (DOJ's) Use of Force orders and policies. TFOs must be briefed on ATF's and DOJ's Use of Force policy by an ATF official, and will be provided with a copy of such policy.

BODY WORN CAMERAS AND TASK FORCE OFFICERS

In accordance with DOJ policy, dated October 29, 2020, Body Worn Cameras (BWCs) may be worn by TFOs operating on a Federal Task Force when their parent agency mandates their use by personnel assigned to the task force. In such cases, the parent agency must formally request to participate in the TFO BWC program and, upon approval, shall comply with all DOJ and ATF policies, and the required procedures, documentation, and reporting while participating on the task force.

In instances where State law and/or agency BWC Policy prevents a parent agency from complying with DOJ and ATF policies, the TFOs operating on a Federal Task Force when their parent agency mandates their use by personnel assigned to the task force shall not participate in the service of search warrants or arrest warrants.

MEDIA

Media relations will be handled by ATF and the U.S. Attorney's Office's public information officers in coordination with each participating agency. Information for press releases will be reviewed and mutually agreed upon by all participating agencies, who will take part in press conferences. Assigned personnel will be informed not to give statements to the media concerning any ongoing investigation or prosecution under this MOU without the concurrence of the other participants and, when appropriate, the relevant prosecutor's office.

All personnel from the participating agencies shall strictly adhere to the requirements of Title 26, United States Code, § 6103. Disclosure of tax return information and tax information acquired during the course of investigations involving National Firearms Act (NFA) firearms as defined in 26 U.S.C., Chapter 53 shall not be made except as provided by law.

SALARY/OVERTIME COMPENSATION

During the period of the MOU, participating agencies will provide for the salary and employment benefits of their respective employees. All participating agencies will retain control over their employees' work hours, including the approval of overtime.

ATF may have funds available to reimburse overtime to the State and Local TFO's agency, subject to the guidelines of the Department of Justice Asset Forfeiture Fund. This funding would be available under the

terms of a memorandum of agreement (MOA) established pursuant to the provisions of 28 U.S.C. section 524. The participating agency agrees to abide by the applicable Federal law and policy with regard to the payment of overtime from the Department of Justice Asset Forfeiture Fund. The participating agency must be recognized under State law as a law enforcement agency and their officers/troopers/investigators as sworn law enforcement officers. If required or requested, the participating agency shall be responsible for demonstrating to the Department of Justice that its personnel are law enforcement officers for the purpose of overtime payment from the Department of Justice Asset Forfeiture Fund. **This MOU is not a funding document.**

In accordance with these provisions and any MOA on asset forfeiture, the ATF Special Agent in Charge or designee shall be responsible for certifying reimbursement requests for overtime expenses incurred as a result of this agreement.

AUDIT INFORMATION

Operations under this MOU are subject to audit by ATF, the Department of Justice's Office of the Inspector General, the Government Accountability Office, and other Government-designated auditors. Participating agencies agree to permit such audits and to maintain all records relating to Department of Justice Asset Forfeiture Fund payments for expenses either incurred during the course of this Task Force or for a period of not less than three (3) years and, if an audit is being conducted, until such time that the audit is officially completed, whichever is greater.

FORFEITURES/SEIZURES

All assets seized for administrative forfeiture will be seized and forfeited in compliance with the rules and regulations set forth by the U.S. Department of Justice Asset Forfeiture guidelines. When the size or composition of the item(s) seized make it impossible for ATF to store it, any of the participating agencies having the storage facilities to handle the seized property agree to store the property at no charge and to maintain the property in the same condition as when it was first taken into custody. The agency storing said seized property agrees not to dispose of the property until authorized to do so by ATF.

The MOU provides that proceeds from forfeitures will be shared, with sharing percentages based upon the U.S. Department of Justice Asset Forfeiture policies on equitable sharing of assets, such as determining the level of involvement by each participating agency. Task Force assets seized through administrative forfeiture will be distributed in equitable amounts based upon the number of full-time persons committed by each participating agency. Should it become impossible to separate the assets into equal shares, it will be the responsibility of all the participating agencies to come to an equitable decision. If this process fails and an impasse results, ATF will become the final arbitrator of the distributive shares for the participating agencies.

DISPUTE RESOLUTION

In cases of overlapping jurisdiction, the participating agencies agree to work in concert to achieve the Task Force's goals and objectives. The parties to this MOU agree to attempt to resolve any disputes regarding jurisdiction, case assignments and workload at the lowest level possible.

LIABILITY

ATF acknowledges that the United States is liable for the wrongful or negligent acts or omissions of its officers and employees, including TFOs, while on duty and acting within the scope of their federal employment, to the extent permitted by the Federal Tort Claims Act.

Claims against the United States for injury or loss of property, personal injury, or death arising or resulting from the negligent or wrongful act or omission of any Federal employee while acting within the scope of his or her office or employment are governed by the Federal Tort Claims Act, 28 U.S.C. sections 1346(b), 2672-2680 (unless the claim arises from a violation of the Constitution of the United States, or a violation of a statute of the United States under which other recovery is authorized).

Except as otherwise provided, the parties agree to be solely responsible for the negligent or wrongful acts or omissions of their respective employees and will not seek financial contributions from the other for such acts or omissions. Legal representation by the United States is determined by the United States Department of Justice on a case-by-case basis. ATF cannot guarantee the United States will provide legal representation to any State or local law enforcement officer.

Liability for any negligent or willful acts of any agent or officer undertaken outside the terms of this MOU will be the sole responsibility of the respective agent or officer and agency involved.

DURATION

This MOU is effective with the signatures of all parties and terminates at the close of business on September 30, 2026.

This MOU supersedes previously signed MOUs and shall remain in effect until the aforementioned expiration date or until it is terminated in writing (to include electronic mail and facsimile), whichever comes first. All participating agencies agree that no agency shall withdraw from the Task Force without providing ninety (90) days written notice to other participating agencies. If any participating agency withdraws from the Task Force prior to its termination, the remaining participating agencies shall determine the distributive share of assets for the withdrawing agency, in accordance with Department of Justice guidelines and directives.

The MOU shall be deemed terminated at the time all participating agencies withdraw and ATF elects not to replace such members, or in the event ATF unilaterally terminates the MOU upon 90 days written notice to all the remaining participating agencies.

MODIFICATIONS

This agreement may be modified at any time by written consent of all participating agencies. Modifications shall have no force and effect unless such modifications are reduced to writing and signed by an authorized representative of each participating agency.

SIGNATURES

_____/_____
Typed Name Date
Title
Department

_____/_____
Vincent C. Pallozzi Date
Special Agent in Charge, ATF
Charlotte Field Division

To: (b) (6), (b) (7)(C)
Cc: (b) (6), (b) (7)(C) (b) (6), (b) (7)(C)
From: Detroit-Operations[(b) (2) @atf.gov]
Sent: Thur 7/15/2021 2:08:37 PM
Subject: RE: ATF BWC Training
ATF Detroit SA Badge Listing July 2021.xlsx

Good morning (b) (6), (b) (7)(C)

I have attached a spreadsheet that includes the Field Offices for Detroit Field Division. For Grand Rapids/Marquette/Lansing, RAC (b) (6), (b) (7)(C) has locked down August 26th (one day is fine) and the training will be held in their new field office conference room which can accommodate around 30. I think we should keep the training at our Division conference room for the Detroit/Flint/Ann Arbor offices for both August 24th and August 25th. I will have (b) (6), (b) (7)(C) send out notices to all of the Divisional and Field Offices when he returns next week but we have secured all of the training sites for now.

(b) (6), (b) (7)(C)

(b) (6), (b) (7)(C)

*Division Operations Officer
Supervisory Special Agent
ATF Detroit Field Division
1155 Brewery Park Blvd. Ste 300
Detroit, MI 48207*

(b) (6), (b) (7)(C) - Office
(b) (6), (b) (7)(C) - Cell

From: (b) (6), (b) (7)(C)
Sent: Wednesday, July 14, 2021 11:31 AM
To: (b) (6), (b) (7)(C)
Cc: (b) (6), (b) (7)(C) (b) (6), (b) (7)(C)
Subject: ATF BWC Training

(b) (6), (b) (7)(C)

Sorry for the confusion here is the corrected training schedule per our conversation. I have cc'd our BWC training coordinator (b) (6), (b) (7)(C) she will be assisting with the training.

Detroit/Ann Arbor/Flint-August 24th-25th in Detroit.

Grand Rapids/Marquette/Lansing-August 26th and 27th (if needed), in Grand Rapids.

We will need a space to accommodate the training which will take 4 hours, We will have an am (8:00am-12:00pm) and a pm training (1:00-5:00) for each location.

Please let me know if this is acceptable.

(b) (6), (b) (7)(C)

Alcohol, Tobacco, Firearms and Explosives

16009 N. 81st Street, Suite 100

Scottsdale, AZ 85260

Special Agent Project Officer-Digital Evidence Management

Technical Project Office

Special Operations Division

(b) (6), (b) (7)(C)

CONFIDENTIALITY NOTICE: E-mail may contain confidential information that is legally privileged. Do not read this e-mail if you are not the intended recipient.

This e-mail transmission, and any documents, files or previous e-mail messages attached to it may contain confidential information that is legally privileged. If you are not the intended recipient, or a person responsible for delivering it to the intended recipient, you are hereby notified that any disclosure, copying, distribution or use of any of the information contained in or attached to this transmission is **STRICTLY PROHIBITED**. If you have received this transmission in error, please immediately notify us by reply e-mail, by forwarding this to **(b) (6), (b) (7)(C)** or by telephone at **(b) (6), (b) (7)(C)** and destroy the original transmission and its attachments without reading or saving in any manner. Thank you.

NATIVE FILE:

ATF Detroit SA Badge Listing July 2021

To: (b) (6), (b) (7)(C)
From: (b) (6), (b) (7)(C)
Sent: Fri 7/30/2021 7:12:53 PM
Subject: RE: Body-Worn Camera Project Budget for FY22
ATF Body Worn Camera Program 07_11_21.docx
15A00021CAQA00021 Axon Enterprise Inc. (Digital Evidence Management Services) (Both Parties Signed).pdf

This is what we provided to (b) (6), (b) (7)(C), Chief of Budge Formulation. These numbers of course depend on congress providing supplemental funding for the ATF body-worn camera/Digital Evidence Management (DEM) Branch Program. The year one costs reflect the cost for 2022 if funding becomes available.

In the event this does not happen we would **not** move forward with the program and only need to continue to support the storage cost for the TFO BWC program and the two ATF divisions currently scheduled to wear BWC's. This is covered in the Axon contract which I have also attached (see year two costs, \$(b) (4)). In addition to the year two cost there would be an ODC training travel budget which would be (b) (4) 0 for additional administrator training as partner agencies continue to onboard TFO's.

Please reach out with any questions!

(b) (6), (b) (7)(C)
Alcohol, Tobacco, Firearms and Explosives
16009 N. 81st Street, Suite 100
Scottsdale, AZ 85260
Special Agent Project Officer-Digital Evidence Management
Technical Project Office
Special Operations Division
(b) (6), (b) (7)(C)

CONFIDENTIALITY NOTICE: E-mail may contain confidential information that is legally privileged. Do not read this e-mail if you are not the intended recipient.

This e-mail transmission, and any documents, files or previous e-mail messages attached to it may contain confidential information that is legally privileged. If you are not the intended recipient, or a person responsible for delivering it to the intended recipient, you are hereby notified that any disclosure, copying, distribution or use of any of the information contained in or attached to this transmission is **STRICTLY PROHIBITED**. If you have received this transmission in error, please immediately notify us by reply e-mail, by forwarding this to (b) (6), (b) (7)(C) or by telephone at (b) (6), (b) (7)(C) and destroy the original transmission and its attachments without reading or saving in any manner. Thank you.

From: (b) (6), (b) (7)(C)
Sent: Friday, July 30, 2021 8:51 AM
To: (b) (6), (b) (7)(C)
Subject: RE: Body-Worn Camera Project Budget for FY22

Thank you!

From: (b) (6), (b) (7)(C)
Sent: Friday, July 30, 2021 11:35 AM
To: (b) (6), (b) (7)(C)
Subject: Re: Body-Worn Camera Project Budget for FY22

No problem, I'll have it to you by COB;)

ATF Senior Special Agent/Digital Evidence Management Systems Project Officer
(b) (6), (b) (7)(C)

On Jul 30, 2021, at 6:54 AM, (b) (6), (b) (7)(C)
(b) (6), (b) (7)(C) wrote:

<image001.gif>

Hi (b) (6), (b) (7)(C)

I recently sent out a request for all branches to submit their FY22 budget requests to me by COB today. This morning as I am going through some of them, it dawned on me that I did not ask you about the body-worn camera project. I was focused on branches and operational expenses under the division, so this project slipped my mind.

I know a couple months back you were working on some costs for OM. Do you have a write-up that you can send me with what you need for the program for FY22 so I can include it in SOD's FY22 budget?

I'm not sitting down with (b) (6), (b) (7)(C) to go over everything until next Friday, so do you think you can have it to me by next Thursday? So sorry for the short notice but it totally slipped my mind. If next Thursday is not doable, please let me know when you can have it to me.

Thanks,

(b) (6), (b) (7)(C)

Bureau of Alcohol, Tobacco, Firearms & Explosives

Office of Field Operations

Special Operations Division

O (b) (6), (b) (7)(C) | C (b) (6), (b) (7)(C)

(b) (6), (b) (7)(C)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24 & 30				1. REQUISITION NUMBER DJA-21-ASOD-PR-0016	
2. CONTRACT NO. 15A00021CAQA00021		3. AWARD/EFFECTIVE DATE 12/13/2020		4. ORDER NUMBER	
7. FOR SOLICITATION INFORMATION CALL:		a. NAME (b) (6), (b) (7)(C)		b. TELEPHONE NUMBER (No collect calls) (O) (b) (6), (b) (7)(C) (F) (b) (6), (b) (7)(C)	
		8. OFFER DUE DATE / LOCAL TIME			
9. ISSUED BY ATF - ACQUISITIONS BRANCH Jim Huff 99 New York Ave. NE Washington, DC 20226		CODE 15A000		10. THE ACQUISITION IS <input checked="" type="checkbox"/> UNRESTRICTED OR <input type="checkbox"/> SET ASIDE: % FOR	
		<input type="checkbox"/> SMALL BUSINESS <input type="checkbox"/> HUBZONE SMALL BUSINESS <input type="checkbox"/> SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS		<input type="checkbox"/> WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM <input type="checkbox"/> EDWOSB NAICS: 334310 SIZE STANDARD: 750 Employees	
11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED <input type="checkbox"/> SEE SCHEDULE		12. DISCOUNT TERMS NET 30		13. RATING	
				14. METHOD OF SOLICITATION <input type="checkbox"/> RFQ <input type="checkbox"/> IFB <input checked="" type="checkbox"/> RFP	
15. DELIVER TO ASSISTANT DIRECTOR - FIELD OPERATIONS ATF 99 New York Ave., NE Room 5.N-621 WASHINGTON, DC 20226		CODE A700000		16. ADMINISTERED BY ATF - Property, Acquisitions and Safety Division (PASD) 99 New York Ave NE WASHINGTON, DC 20226	
17a. CONTRACTOR/OFFEROR AXON ENTERPRISE, INC. 17800 N 85TH ST SCOTTSDALE, AZ 85255-6311 DUNS: 832176382		CODE 860741227 FACILITY CODE 832176382		18a. PAYMENT WILL BE MADE BY ATF - Finance Branch 99 New York Avenue NE, #4.S-288 Washington, DC 20226	
				CODE A404040 (b) (2) @ATF.gov	
TELEPHONE NO. (480) 905-2088		17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER <input type="checkbox"/>		18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED <input type="checkbox"/> SEE ADDENDUM	
19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES		21. QUANTITY	22. UNIT	23. UNIT PRICE
	Delivery Date: 12/12/2025 This contract incorporates quote Q-256699 and the associated terms in full. Axon Enterprise, Inc. POC (b) (6), (b) (7)(C) E-Mail (b) (6), (b) (7)(C) PH# (b) (6), (b) (7)(C) See Continuation Sheet(s) (Use Reverse and/or Attach Additional Sheets as Necessary)				
25. ACCOUNTING AND APPROPRIATION DATA See Lines					26. TOTAL AWARD AMOUNT (For Govt. Use Only) \$1,305,000.00
27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA <input type="checkbox"/> ARE <input type="checkbox"/> ARE NOT ATTACHED			27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA <input checked="" type="checkbox"/> ARE <input type="checkbox"/> ARE NOT ATTACHED		
28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN 1 COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED			29. AWARD OF CONTRACT: REF. Q-256699 OFFER DATED 11/03/2020. YOUR OFFER ON SOLICITATION (BLOCK 5) INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS: Entirety		
30a. SIGNATURE OF OFFEROR/CONTRACTOR (b) (6), (b) (7)(C)			31a. UNITED STATES OF AMERICA (SIGNATURE OF CONTRACTING OFFICER) JAMES HUFF Digitally signed by JAMES HUFF Date: 2020.12.02 14:19:30 -0500		
30b. NAME AND TITLE OF SIGNER (TYPE OR PRINT) Richard Coleman VP/GM, Federal Sector		30c. DATE SIGNED 12/2/2020		31b. NAME OF THE CONTRACTING OFFICER (TYPE OR PRINT) James M. Huff	
				31c. DATE SIGNED	

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT

32a. QUANTITY IN COLUMN 21 HAS BEEN

☐ RECEIVED ☐ INSPECTED ☐ ACCEPTED, AND CONFORMS TO THE CONTRACT, EXCEPT AS NOTED: _____

32b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE		32c. DATE	32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE		
32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE			32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE		
			32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE		
33. SHIP NUMBER		34. VOUCHER NUMBER	35. AMOUNT VERIFIED CORRECT FOR	36. PAYMENT <input type="checkbox"/> COMPLETE <input type="checkbox"/> PARTIAL <input type="checkbox"/> FINAL	37. CHECK NUMBER
<input type="checkbox"/> PARTIAL <input type="checkbox"/> FINAL					
38. S/R ACCOUNT NUMBER	39. S/R VOUCHER NUMBER	40. PAID BY			
41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT		42a. RECEIVED BY (Print)			
41b. SIGNATURE AND TITLE OF CERTIFYING OFFICER		41c. DATE	42b. RECEIVED AT (Location)		
			42c. DATE REC'D (YY/MM/DD)		
			42d. TOTAL CONTAINERS		

Table of Contents

<u>Section</u>	<u>Description</u>	<u>Page Number</u>
1	Solicitation/Contract Form.....	1
2	Commodity or Services Schedule.....	5
	Section B Supplies or Services and Prices/Costs.....	8
3	Contract Clauses.....	10
	Section C Descriptions and Specifications.....	14
	52.246-2 Inspection of Supplies-Fixed-Price (Aug 1996).....	14
	52.246-4 Inspection of Services-Fixed-Price (Aug 1996).....	15
	ATF-01 ACCESSIBILITY OF ELECTRONIC AND INFORMATION TECHNOLOGY (SECTION 508).....	16
	ATF-03 SECTION 508 TECHNICAL REQUIREMENTS.....	16
	ATF-12 NON-US CITIZENS PROHIBITED FROM ACCESS TO DOJ INFORMATION TECHNOLOGY (IT) SYSTEMS.....	23
	ATF-14 ELECTRONIC INVOICING.....	23
	ATF-17 NOTICE TO THE GOVERNMENT OF DELAYS.....	24
	ATF-18 REQUIREMENTS FOR ACCESS TO LAW ENFORCEMENT SENSITIVE INFORMATION.....	24
	ATF-19 AUTHORITY TO OBLIGATE THE GOVERNMENT.....	24
	ATF-21 ALL ITEMS TO BECOME THE PROPERTY OF THE GOVERNMENT.....	24
	ATF-22 CONFIDENTIALITY OF INFORMATION AND DISCLOSURE.....	25
	ATF-23 PRIVACY OR SECURITY SAFEGUARDS.....	26
	ATF-24 COMPUTER SECURITY.....	26
	ATF-27 INFORMATION RESELLERS OR DATA BROKERS.....	27
	ATF-28 CONTRACTOR CERTIFICATION OF COMPLIANCE WITH FEDERAL TAX REQUIREMENTS.....	27
	ATF-30 COMMON SECURITY CONFIGURATIONS.....	27
	ATF-35 52.232-99, Providing Accelerated Payment to Small Business Subcontractors (DEVIATION) (AUG 2012).....	28
	ATF-38 Representation Regarding Acquisition by Lease, Purchase or Otherwise of any Equipment or Software (November 2013).....	28
	ATF-41 DEPARTMENT POLICY ON DOMESTIC VIOLENCE, SEXUAL ASSAULT, AND STALKING.....	29
	ATF-46 Corporate Representation Regarding Felony Conviction Under Any Federal Law or Unpaid Delinquent Tax Liability - Award (DEVIATION 2015-02) (March 2015).....	29
	ATF-47 Contractor Internal Confidentiality Agreements or Statements Prohibiting or Restricting Reporting of Waste, Fraud, and Abuse - Award (DEVIATION 2015-02) (March 2015).....	29
	ATF-48 Contractor Certification of Compliance with Federal Tax Requirements - Award (DEVIATION 2015-02) (March 2015).....	30
	ATF-49 ATF-49 SECURITY OF INFORMATION AND INFORMATION SYSTEMS, INCLUDING PERSONALLY-IDENTIFIABLE DATA (PII) (Revised April 8, 2016).....	30
	Section H Special Contract Requirements (ATF & DOJ Clauses).....	36
	52.203-3 Gratuities (Apr 1984).....	38
	52.203-5 Covenant Against Contingent Fees (May 2014).....	39
	52.203-7 Anti-Kickback Procedures (May 2014).....	39
	52.203-12 Limitation On Payments To Influence Certain Federal Transactions (Oct 2010).....	40
	52.203-17 Contractor Employee Whistleblower Rights and Requirement To Inform Employees of Whistleblower Rights (Apr 2014).....	43
	52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (Aug 2019).....	43
	52.212-4 Contract Terms and Conditions-Commercial Items (Oct 2018).....	
	52.212-5 Contract Terms and Conditions Required to Implement Statutes or Executive Orders--Commercial Items (Oct 2019).....	
	52.215-19 Notification of Ownership Changes (Oct 1997).....	45
	52.217-8 Option to Extend Services (Nov 1999).....	45
	52.227-1 Authorization and Consent (Dec 2007).....	46
	52.227-2 Notice and Assistance Regarding Patent and Copyright Infringement (Dec 2007).....	46
	52.227-14 Rights in Data-General (May 2014).....	46

52.229-4 Federal, State and Local Taxes (State and Local Adjustments) (Feb 2013).....	50
52.232-1 Payments (Apr 1984).....	51
52.232-39 Unenforceability of Unauthorized Obligations (Jun 2013).....	51
52.233-3 Protest after Award (Aug 1996).....	51
52.233-3 Alt I Protest after Award (Aug 1996) - Alternate I (Jun 1985).....	52
52.242-1 Notice of Intent to Disallow Costs (Apr 1984).....	53
52.243-1 Changes-Fixed-Price (Aug 1987).....	53
52.243-1 Alt II Changes-Fixed-Price (Aug 1987) - Alternate II (Apr 1984).....	54
52.246-24 Limitation of Liability-High-Value Items (Feb 1997).....	54
52.249-2 Termination for Convenience of the Government (Fixed-Price) (Apr 2012).....	55
52.249-8 Default (Fixed-Price Supply and Service) (Apr 1984).....	57
52.249-8 Alt I Default (Fixed-Price Supply and Service) (Apr 1984) - Alternate I (Apr 1984).....	58

Section 2 - Commodity or Services Schedule

Contract Guarantee:

Minimum Guaranteed Quantity	Minimum Guaranteed Amount	Maximum Guaranteed Quantity	Maximum Guaranteed Amount
	\$1,275,000.00		\$1,275,000.00

SCHEDULE OF SUPPLIES/SERVICES

CONTINUATION SHEET

ITEM NO.	SUPPLIES/SERVICES	MAX. QUANTITY	UNIT	UNIT PRICE	AMOUNT
0001	Base Year Digital Evidence Mgt Software (DEMS) Services: The contractor shall provide DEMS Services: Licenses, Storage, and Maintenance Support for the Digital Evidence Management Program Firm Fixed Price PSC: 5836 Line Period of Performance: 12/13/2020 - 12/12/2021 Base Period	1	LT	Previous: \$0.0000 Change: \$1,275,000.0000 Current: \$1,275,000.0000	Previous: \$0.00 Change: \$1,275,000.00 Current: \$1,275,000.00
0002	Base Year Other Direct Costs (ODCs) will be, but not limited, to additional Material to include body worn cameras; migration services; additional accessories, additional Software and additional Training. Funding will not exceed \$250,000 for the Base Year. Funding must be provided before ODCs can be procured. Firm Fixed Price PSC: 5836 Line Period of Performance: 12/13/2020 - 12/12/2021 Base Period	1	LT	Previous: \$0.0000 Change: \$30,000.0000 Current: \$30,000.0000	Previous: \$0.00 Change: \$30,000.00 Current: \$30,000.00
1001	Option Period One Digital Evidence Mgt Software (DEMS) Services: The contractor shall provide DEMS Services: Licenses, Storage, and Maintenance Support for the Digital Evidence Management Program Firm Fixed Price PSC: 5836 Line Period of Performance: 12/13/2021 - 12/12/2022 Unexercised Option	1	LT	Previous: \$0.0000 Change: (b) (4) Current: (b) (4)	Previous: \$0.00 Change: (b) (4) Current: (b) (4)

ITEM NO.	SUPPLIES/SERVICES	MAX. QUANTITY	UNIT	UNIT PRICE	AMOUNT
1002	<p>Option Period One</p> <p>Other Direct Costs (ODCs) will be, but not limited, to additional Material to include body worn camerascameras; migration services; additional accessories, additional Software and additional Training. Funding will not exceed \$250,000 per Option Year. Funding must be provided before ODCs can be procured.</p> <p>Firm Fixed Price</p> <p>PSC: 5836</p> <p>Line Period of Performance: 12/13/2021 - 12/12/2022</p> <p>Unexercised Option</p>	1	LT	<p>Previous:</p> <p>\$0.0000</p> <p>Change:</p> <p>(b) (4)</p> <p>Current:</p> <p>(b) (4)</p>	<p>Previous: \$0.00</p> <p>Change: (b) (4)</p> <p>Current: (b) (4)</p>
ITEM NO.	SUPPLIES/SERVICES	MAX. QUANTITY	UNIT	UNIT PRICE	AMOUNT
2001	<p>Option Period Two</p> <p>Digital Evidence Mgt Software (DEMS) Services: The contractor shall provide DEMS Services: Licenses, Storage, and Maintenance Support for the Digital Evidence Management Program</p> <p>Firm Fixed Price</p> <p>PSC: 5836</p> <p>Line Period of Performance: 12/13/2022 - 12/12/2023</p> <p>Unexercised Option</p>	1	LT	<p>Previous:</p> <p>\$0.0000</p> <p>Change:</p> <p>(b) (4)</p> <p>Current:</p> <p>(b) (4)</p>	<p>Previous: \$0.00</p> <p>Change: (b) (4)</p> <p>Current: (b) (4)</p>
ITEM NO.	SUPPLIES/SERVICES	MAX. QUANTITY	UNIT	UNIT PRICE	AMOUNT
2002	<p>Option Period Two</p> <p>Other Direct Costs (ODCs) will be, but not limited, to additional Material to include body worn camerascameras; migration services; additional accessories, additional Software and additional Training. Funding will not exceed \$250,000 per Option Year. Funding must be provided before ODCs can be procured.</p> <p>Firm Fixed Price</p> <p>PSC: 5836</p> <p>Line Period of Performance: 12/13/2022 - 12/12/2023</p> <p>Unexercised Option</p>	1	LT	<p>Previous:</p> <p>\$0.0000</p> <p>Change:</p> <p>(b) (4)</p> <p>Current:</p> <p>(b) (4)</p>	<p>Previous: \$0.00</p> <p>Change: (b) (4)</p> <p>Current: (b) (4)</p>
ITEM NO.	SUPPLIES/SERVICES	MAX. QUANTITY	UNIT	UNIT PRICE	AMOUNT
3001	<p>Option Period Three</p> <p>Digital Evidence Mgt Software (DEMS) Services: The contractor shall provide DEMS Services: Licenses, Storage, and Maintenance Support for the Digital Evidence Management Program</p> <p>Firm Fixed Price</p> <p>PSC: 5836</p> <p>Line Period of Performance: 12/13/2023 - 12/12/2024</p> <p>Unexercised Option</p>	1	LT	<p>Previous:</p> <p>\$0.0000</p> <p>Change:</p> <p>(b) (4)</p> <p>Current:</p> <p>(b) (4)</p>	<p>Previous: \$0.00</p> <p>Change: (b) (4)</p> <p>Current: (b) (4)</p>

ITEM NO.	SUPPLIES/SERVICES	MAX. QUANTITY	UNIT	UNIT PRICE	AMOUNT
3002	Option Period Three Other Direct Costs (ODCs) will be, but not limited, to additional Material to include body worn camerascameras; migration services; additional accessories, additional Software and additional Training. Funding will not exceed \$250,000 per Option Year. Funding must be provided before ODCs can be procured. Firm Fixed Price PSC: 5836 Line Period of Performance: 12/13/2023 - 12/12/2024 Unexercised Option	1	LT	Previous: \$0.0000 Change: (b) (4) Current: (b) (4)	Previous: \$0.00 Change: (b) (4) Current: (b) (4)
ITEM NO.	SUPPLIES/SERVICES	MAX. QUANTITY	UNIT	UNIT PRICE	AMOUNT
4001	Option Period Four Digital Evidence Mgt Software (DEMS) Services: The contractor shall provide DEMS Services: Licenses, Storage, and Maintenance Support for the Digital Evidence Management Program Firm Fixed Price PSC: 5836 Line Period of Performance: 12/13/2024 - 12/12/2025 Unexercised Option	1	LT	Previous: \$0.0000 Change: (b) (4) Current: (b) (4)	Previous: \$0.00 Change: (b) (4) Current: (b) (4)
ITEM NO.	SUPPLIES/SERVICES	MAX. QUANTITY	UNIT	UNIT PRICE	AMOUNT
4002	Option Period Four Other Direct Costs (ODCs) will be, but not limited, to additional Material to include body worn camerascameras; migration services; additional accessories, additional Software and additional Training. Funding will not exceed \$250,000 per Option Year. Funding must be provided before ODCs can be procured. Firm Fixed Price PSC: 5836 Line Period of Performance: 12/13/2024 - 12/12/2025 Unexercised Option	1	LT	Previous: \$0.0000 Change: (b) (4) Current: (b) (4)	Previous: \$0.00 Change: (b) (4) Current: (b) (4)
Base Total:					\$1,305,000.00
Exercised Options Total:					\$0.00
Unexercised Options Total:					(b) (4)
Base and Options Total:					(b) (4)

FUNDING DETAILS:

ITEM NO.	FUNDING LINE	OBLIGATED AMOUNT	ACCOUNTING CODES
0001	1	\$1,275,000.00	ATF-2021-700D-FO-701200-LEO-G1P-25218-2021
0002	1	\$30,000.00	ATF-2021-700D-FO-701200-LEO-G1P-25218-2021

TOTAL: \$1,305,000.00

ATF COR (b) (6), (b) (7)(C)

Cell# (b) (6), (b) (7)(C)

PH# (b) (6), (b) (7)(C)

ATF POC (b) (6), (b) (7)(C)

Cell# (b) (6), (b) (7)(C)

Section B Supplies or Services and Prices/Costs

The Bureau of Alcohol, Tobacco, Firearms and Explosives intends on awarding a Firm Fixed Price type contract to acquire Digital Evidence Management Services: Software, Storage, and Maintenance Support for the Special Operation Division under the Field Operation Directorate.

B.1 SUPPLIES / SERVICES BEING PROCURED

The Contractor shall provide support for the Digital Evidence Management Services: Software, Storage, and Maintenance Support in accordance with the specifications outlined in the Statement of Work (SOW) under Section C of this RFP.

B.2 CONTRACT TYPE

This will be a Firm Fixed Price type contract.

B.3 PERIOD OF PERFORMANCE

The period of performance of the contract shall be for a one (1) year base period with the option to extend the period of performance for up to four (4) additional twelve (12) month periods at the Government's discretion. Overall contract will Not to Exceed five (5) years or sixty (66) months, if FAR Part Clause 52.217-8 Option to Extend Services is used.

B.4 SCHEDULE

B.4 SCHEDULE

BASE PERIOD: 12/13/2020 thru 12/12/2021

OPTION PERIOD ONE: 12/13/2021 thru 12/12/2022

OPTION PERIOD TWO: 12/13/2022 thru 12/12/2023

OPTION PERIOD THREE: 12/13/2023 thru 12/12/2024

OPTION PERIOD FOUR: 12/13/2024 thru 12/12/2025

Section 3 - Contract Clauses

52.212-4 Contract Terms and Conditions-Commercial Items (Oct 2018)

(a) *Inspection/Acceptance.* The Contractor shall only tender for acceptance those items that conform to the requirements of this contract. The Government reserves the right to inspect or test any supplies or services that have been tendered for acceptance. The Government may require repair or replacement of nonconforming supplies or reperformance of nonconforming services at no increase in contract price. If repair/replacement or reperformance will not correct the defects or is not possible, the Government may seek an equitable price reduction or adequate consideration for acceptance of nonconforming supplies or services. The Government must exercise its post-acceptance rights--

(1) Within a reasonable time after the defect was discovered or should have been discovered; and

(2) Before any substantial change occurs in the condition of the item, unless the change is due to the defect in the item.

(b) *Assignment.* The Contractor or its assignee may assign its rights to receive payment due as a result of performance of this contract to a bank, trust company, or other financing institution, including any Federal lending agency in accordance with the Assignment of Claims Act (31 U.S.C. 3727). However, when a third party makes payment (*e.g.*, use of the Governmentwide commercial purchase card), the Contractor may not assign its rights to receive payment under this contract.

(c) *Changes.* Changes in the terms and conditions of this contract may be made only by written agreement of the parties.

(d) *Disputes.* This contract is subject to 41 U.S.C. chapter 71, Contract Disputes. Failure of the parties to this contract to reach agreement on any request for equitable adjustment, claim, appeal or action arising under or relating to this contract shall be a dispute to be resolved in accordance with the clause at FAR 52.233-1, Disputes, which is incorporated herein by reference. The Contractor shall proceed diligently with performance of this contract, pending final resolution of any dispute arising under the contract.

(e) *Definitions.* The clause at FAR 52.202-1, Definitions, is incorporated herein by reference.

(f) *Excusable delays.* The Contractor shall be liable for default unless nonperformance is caused by an occurrence beyond the reasonable control of the Contractor and without its fault or negligence such as, acts of God or the public enemy, acts of the Government in either its sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, unusually severe weather, and delays of common carriers. The Contractor shall notify the Contracting Officer in writing as soon as it is reasonably possible after the commencement of any excusable delay, setting forth the full particulars in connection therewith, shall remedy such occurrence with all reasonable dispatch, and shall promptly give written notice to the Contracting Officer of the cessation of such occurrence.

(g) *Invoice.*

(1) The Contractor shall submit an original invoice and three copies (or electronic invoice, if authorized) to the address designated in the contract to receive invoices. An invoice must include--

(i) Name and address of the Contractor;

(ii) Invoice date and number;

(iii) Contract number, line item number and, if applicable, the order number;

(iv) Description, quantity, unit of measure, unit price and extended price of the items delivered;

(v) Shipping number and date of shipment, including the bill of lading number and weight of shipment if shipped on Government bill of lading;

(vi) Terms of any discount for prompt payment offered;

(vii) Name and address of official to whom payment is to be sent;

(viii) Name, title, and phone number of person to notify in event of defective invoice; and

(ix) Taxpayer Identification Number (TIN). The Contractor shall include its TIN on the invoice only if required elsewhere in this contract.

(x) Electronic funds transfer (EFT) banking information.

(A) The Contractor shall include EFT banking information on the invoice only if required elsewhere in this contract.

(B) If EFT banking information is not required to be on the invoice, in order for the invoice to be a proper invoice, the Contractor shall have submitted correct EFT banking information in accordance with the applicable solicitation provision, contract clause (*e.g.*, 52.232-33, Payment by Electronic Funds Transfer--System for Award Management, or 52.232-34, Payment by Electronic Funds Transfer--Other Than System for Award Management), or applicable agency procedures.

(C) EFT banking information is not required if the Government waived the requirement to pay by EFT.

(2) Invoices will be handled in accordance with the Prompt Payment Act (31 U.S.C. 3903) and Office of Management and Budget (OMB) prompt payment regulations at 5 CFR Part 1315.

(h) *Patent indemnity.* The Contractor shall indemnify the Government and its officers, employees and agents against liability, including costs, for actual or alleged direct or contributory infringement of, or inducement to infringe, any United States or foreign patent, trademark or copyright, arising out of the performance of this contract, provided the Contractor is reasonably notified of such claims and proceedings.

(i) *Payment.--*

(1) *Items accepted.* Payment shall be made for items accepted by the Government that have been delivered to the delivery destinations set forth in this contract.

(2) *Prompt payment.* The Government will make payment in accordance with the Prompt Payment Act (31 U.S.C. 3903) and prompt payment regulations at 5 CFR Part 1315.

(3) *Electronic Funds Transfer (EFT).* If the Government makes payment by EFT, see 52.212-5(b) for the appropriate EFT clause.

(4) *Discount.* In connection with any discount offered for early payment, time shall be computed from the date of the invoice. For the purpose of computing the discount earned, payment shall be considered to have been made on the date which appears on the payment check or the specified payment date if an electronic funds transfer payment is made.

(5) *Overpayments.* If the Contractor becomes aware of a duplicate contract financing or invoice payment or that the Government has otherwise overpaid on a contract financing or invoice payment, the Contractor shall--

(i) Remit the overpayment amount to the payment office cited in the contract along with a description of the overpayment including the--

(A) Circumstances of the overpayment (*e.g.*, duplicate payment, erroneous payment, liquidation errors, date(s) of overpayment);

(B) Affected contract number and delivery order number, if applicable;

(C) Affected line item or subline item, if applicable; and

(D) Contractor point of contact.

(ii) Provide a copy of the remittance and supporting documentation to the Contracting Officer.

(6) *Interest.*

(i) All amounts that become payable by the Contractor to the Government under this contract shall bear simple interest from the date due until paid unless paid within 30 days of becoming due. The interest rate shall be the interest rate established by the Secretary of the Treasury as provided in 41 U.S.C. 7109, which is applicable to the period in which the amount becomes due, as provided in (i)(6) of this clause, and then at the rate applicable for each six-month period as fixed by the Secretary until the amount is paid.

(ii) The Government may issue a demand for payment to the Contractor upon finding a debt is due under the contract.

(iii) *Final decisions.* The Contracting Officer will issue a final decision as required by 33.211 if--

(A) The Contracting Officer and the Contractor are unable to reach agreement on the existence or amount of a debt within 30 days;

(B) The Contractor fails to liquidate a debt previously demanded by the Contracting Officer within the timeline specified in the demand for payment unless the amounts were not repaid because the Contractor has requested an installment payment agreement; or

(C) The Contractor requests a deferment of collection on a debt previously demanded by the Contracting Officer (see 32.607-2).

(iv) If a demand for payment was previously issued for the debt, the demand for payment included in the final decision shall identify the same due date as the original demand for payment.

(v) Amounts shall be due at the earliest of the following dates:

(A) The date fixed under this contract.

(B) The date of the first written demand for payment, including any demand for payment resulting from a default termination.

(vi) The interest charge shall be computed for the actual number of calendar days involved beginning on the due date and ending on--

(A) The date on which the designated office receives payment from the Contractor;

(B) The date of issuance of a Government check to the Contractor from which an amount otherwise payable has been withheld as a credit against the contract debt; or

(C) The date on which an amount withheld and applied to the contract debt would otherwise have become payable to the Contractor.

(vii) The interest charge made under this clause may be reduced under the procedures prescribed in 32.608-2 of the Federal Acquisition Regulation in effect on the date of this contract.

(j) *Risk of loss.* Unless the contract specifically provides otherwise, risk of loss or damage to the supplies provided under this contract shall remain with the Contractor until, and shall pass to the Government upon:

(1) Delivery of the supplies to a carrier, if transportation is f.o.b. origin; or

(2) Delivery of the supplies to the Government at the destination specified in the contract, if transportation is f.o.b. destination.

(k) *Taxes.* The contract price includes all applicable Federal, State, and local taxes and duties.

(l) *Termination for the Government's convenience.* The Government reserves the right to terminate this contract, or any part hereof, for its sole convenience. In the event of such termination, the Contractor shall immediately stop all work hereunder and shall immediately cause any and all of its suppliers and subcontractors to cease work. Subject to the terms of this contract, the Contractor shall be paid a percentage of the contract price reflecting the percentage of the work performed prior to the notice of termination, plus reasonable charges the Contractor can demonstrate to the satisfaction of the Government using its standard record keeping system, have resulted from the termination. The Contractor shall not be required to comply with the cost accounting standards or contract cost principles for this purpose. This paragraph does not give the Government any right to audit the Contractor's records. The Contractor shall not be paid for any work performed or costs incurred which reasonably could have been avoided.

(m) *Termination for cause.* The Government may terminate this contract, or any part hereof, for cause in the event of any default by the Contractor, or if the Contractor fails to comply with any contract terms and conditions, or fails to provide the Government, upon request, with adequate assurances of future performance. In the event of termination for cause, the Government shall not be liable to the Contractor for any amount for supplies or services not accepted, and the Contractor shall be liable to the Government for any and all rights and remedies provided by law. If it is determined that the Government improperly terminated this contract for default, such termination shall be deemed a termination for convenience.

(n) *Title.* Unless specified elsewhere in this contract, title to items furnished under this contract shall pass to the Government upon acceptance, regardless of when or where the Government takes physical possession.

(o) *Warranty*. The Contractor warrants and implies that the items delivered hereunder are merchantable and fit for use for the particular purpose described in this contract.

(p) *Limitation of liability*. Except as otherwise provided by an express warranty, the Contractor will not be liable to the Government for consequential damages resulting from any defect or deficiencies in accepted items.

(q) *Other compliances*. The Contractor shall comply with all applicable Federal, State and local laws, executive orders, rules and regulations applicable to its performance under this contract.

(r) *Compliance with laws unique to Government contracts*. The Contractor agrees to comply with 31 U.S.C. 1352 relating to limitations on the use of appropriated funds to influence certain Federal contracts; 18 U.S.C. 431 relating to officials not to benefit; 40 U.S.C. chapter 37, Contract Work Hours and Safety Standards; 41 U.S.C. chapter 87, Kickbacks; 41 U.S.C. 4712 and 10 U.S.C. 2409 relating to whistleblower protections; 49 U.S.C. 40118, Fly American; and 41 U.S.C. chapter 21 relating to procurement integrity.

(s) *Order of precedence*. Any inconsistencies in this solicitation or contract shall be resolved by giving precedence in the following order:

(1) The schedule of supplies/services.

(2) The Assignments, Disputes, Payments, Invoice, Other Compliances, Compliance with Laws Unique to Government Contracts, and Unauthorized Obligations paragraphs of this clause;

(3) The clause at 52.212-5.

(4) Addenda to this solicitation or contract, including any license agreements for computer software.

(5) Solicitation provisions if this is a solicitation.

(6) Other paragraphs of this clause.

(7) The Standard Form 1449.

(8) Other documents, exhibits, and attachments.

(9) The specification.

(t) [Reserved]

(u) *Unauthorized Obligations*

(1) Except as stated in paragraph (u)(2) of this clause, when any supply or service acquired under this contract is subject to any End User License Agreement (EULA), Terms of Service (TOS), or similar legal instrument or agreement, that includes any clause requiring the Government to indemnify the Contractor or any person or entity for damages, costs, fees, or any other loss or liability that would create an Anti-Deficiency Act violation (31 U.S.C. 1341), the following shall govern:

(i) Any such clause is unenforceable against the Government.

(ii) Neither the Government nor any Government authorized end user shall be deemed to have agreed to such clause by virtue of it appearing in the EULA, TOS, or similar legal instrument or agreement. If the EULA, TOS, or similar legal instrument or agreement is invoked through an "I agree" click box or other comparable mechanism (e.g., "click-wrap" or "browse-wrap" agreements), execution does not bind the Government or any Government authorized end user to such clause.

(iii) Any such clause is deemed to be stricken from the EULA, TOS, or similar legal instrument or agreement.

(2) Paragraph (u)(1) of this clause does not apply to indemnification by the Government that is expressly authorized by statute and specifically authorized under applicable agency regulations and procedures.

(v) *Incorporation by reference*. The Contractor's representations and certifications, including those completed electronically via the System for Award Management (SAM), are incorporated by reference into the contract.

(End of clause)

A.1 ADDENDUM TO FAR 52.212-4, Limitation On Payments To Influence Certain Federal Transactions (Oct 2010)

The terms and conditions for the following clauses are hereby incorporated into this solicitation and resulting contract as an addendum to FAR clause 52.212-4.

Clauses By Full Text

Section C Descriptions and Specifications

The Contractor shall furnish the necessary personnel, material, equipment, services and facilities (except as otherwise specified), to perform the Statement of Work (SOW) / Specifications as well as all the attachment identified below. These documents are fully incorporated in this contract. All of the terms/conditions as well as clauses entered by the Government supersedes any terms/conditions provided by the Contractor as identified in the Quote with Pricing List and Terms/Conditions listed in Attachment 2.

Attachment 1 - SOW for Digital Evidence Management Services

Attachment 2 - Quote with Pricing List and Terms/Conditions

52.246-2 Inspection of Supplies-Fixed-Price (Aug 1996)

(a) *Definition.* "Supplies," as used in this clause, includes but is not limited to raw materials, components, intermediate assemblies, end products, and lots of supplies.

(b) The Contractor shall provide and maintain an inspection system acceptable to the Government covering supplies under this contract and shall tender to the Government for acceptance only supplies that have been inspected in accordance with the inspection system and have been found by the Contractor to be in conformity with contract requirements. As part of the system, the Contractor shall prepare records evidencing all inspections made under the system and the outcome. These records shall be kept complete and made available to the Government during contract performance and for as long afterwards as the contract requires. The Government may perform reviews and evaluations as reasonably necessary to ascertain compliance with this paragraph. These reviews and evaluations shall be conducted in a manner that will not unduly delay the contract work. The right of review, whether exercised or not, does not relieve the Contractor of the obligations under the contract.

(c) The Government has the right to inspect and test all supplies called for by the contract, to the extent practicable, at all places and times, including the period of manufacture, and in any event before acceptance. The Government shall perform inspections and tests in a manner that will not unduly delay the work. The Government assumes no contractual obligation to perform any inspection and test for the benefit of the Contractor unless specifically set forth elsewhere in this contract.

(d) If the Government performs inspection or test on the premises of the Contractor or a subcontractor, the Contractor shall furnish, and shall require subcontractors to furnish, at no increase in contract price, all reasonable facilities and assistance for the safe and convenient performance of these duties. Except as otherwise provided in the contract, the Government shall bear the expense of Government inspections or tests made at other than the Contractor's or subcontractor's premises; provided, that in case of rejection, the Government shall not be liable for any reduction in the value of inspection or test samples.

(e)(1) When supplies are not ready at the time specified by the Contractor for inspection or test, the Contracting Officer may charge to the Contractor the additional cost of inspection or test.

(2) The Contracting Officer may also charge the Contractor for any additional cost of inspection or test when prior rejection makes reinspection or retest necessary.

(f) The Government has the right either to reject or to require correction of nonconforming supplies. Supplies are nonconforming when they are defective in material or workmanship or are otherwise not in conformity with contract requirements. The Government may reject nonconforming supplies with or without disposition instructions.

(g) The Contractor shall remove supplies rejected or required to be corrected. However, the Contracting Officer may require or permit correction in place, promptly after notice, by and at the expense of the Contractor. The Contractor shall not tender for acceptance corrected or rejected supplies without disclosing the former rejection or requirement for correction, and, when required, shall disclose the corrective action taken.

(h) If the Contractor fails to promptly remove, replace, or correct rejected supplies that are required to be removed or to be replaced or corrected, the Government may either (1) by contract or otherwise, remove, replace, or correct the supplies and charge the cost to the Contractor or (2) terminate the contract for default. Unless the Contractor corrects or replaces the supplies within the delivery schedule, the Contracting Officer may require their delivery and make an equitable price reduction. Failure to agree to a price reduction shall be a dispute.

(i)(1) If this contract provides for the performance of Government quality assurance at source, and if requested by the Government, the Contractor shall furnish advance notification of the time--

(i) When Contractor inspection or tests will be performed in accordance with the terms and conditions of the contract; and

(ii) When the supplies will be ready for Government inspection.

(2) The Government's request shall specify the period and method of the advance notification and the Government representative to whom it shall be furnished. Requests shall not require more than 2 workdays of advance notification if the Government representative is in residence in the Contractor's plant, nor more than 7 workdays in other instances.

(j) The Government shall accept or reject supplies as promptly as practicable after delivery, unless otherwise provided in the contract. Government failure to inspect and accept or reject the supplies shall not relieve the Contractor from responsibility, nor impose liability on the Government, for nonconforming supplies.

(k) Inspections and tests by the Government do not relieve the Contractor of responsibility for defects or other failures to meet contract requirements discovered before acceptance. Acceptance shall be conclusive, except for latent defects, fraud, gross mistakes amounting to fraud, or as otherwise provided in the contract.

(l) If acceptance is not conclusive for any of the reasons in paragraph (k) hereof, the Government, in addition to any other rights and remedies provided by law, or under other provisions of this contract, shall have the right to require the Contractor (1) at no increase in contract price, to correct or replace the defective or nonconforming supplies at the original point of delivery or at the Contractor's plant at the Contracting Officer's election, and in accordance with a reasonable delivery schedule as may be agreed upon between the Contractor and the Contracting Officer; provided, that the Contracting Officer may require a reduction in contract price if the Contractor fails to meet such delivery schedule, or (2) within a reasonable time after receipt by the Contractor of notice of defects or nonconformance, to repay such portion of the contract as is equitable under the circumstances if the Contracting Officer elects not to require correction or replacement. When supplies are returned to the Contractor, the Contractor shall bear the transportation cost from the original point of delivery to the Contractor's plant and return to the original point when that point is not the Contractor's plant. If the Contractor fails to perform or act as required in paragraph (l)(1) or (l)(2) of this clause and does not cure such failure within a period of 10 days (or such longer period as the Contracting Officer may authorize in writing) after receipt of notice from the Contracting Officer specifying such failure, the Government shall have the right by contract or otherwise to replace or correct such supplies and charge to the Contractor the cost occasioned the Government thereby.

(End of clause)

52.246-4 Inspection of Services-Fixed-Price (Aug 1996)

(a) *Definition.* "Services," as used in this clause, includes services performed, workmanship, and material furnished or utilized in the performance of services.

(b) The Contractor shall provide and maintain an inspection system acceptable to the Government covering the services under this contract. Complete records of all inspection work performed by the Contractor shall be maintained and made available to the Government during contract performance and for as long afterwards as the contract requires.

(c) The Government has the right to inspect and test all services called for by the contract, to the extent practicable at all times and places during the term of the contract. The Government shall perform inspections and tests in a manner that will not unduly delay the work.

(d) If the Government performs inspections or tests on the premises of the Contractor or a subcontractor, the Contractor shall furnish, and shall require subcontractors to furnish, at no increase in contract price, all reasonable facilities and assistance for the safe and convenient performance of these duties.

(e) If any of the services do not conform with contract requirements, the Government may require the Contractor to perform the services again in conformity with contract requirements, at no increase in contract amount. When the defects in services cannot be corrected by reperformance, the Government may--

(1) Require the Contractor to take necessary action to ensure that future performance conforms to contract requirements; and

(2) Reduce the contract price to reflect the reduced value of the services performed.

(f) If the Contractor fails to promptly perform the services again or to take the necessary action to ensure future performance in conformity with contract requirements, the Government may--

(1) By contract or otherwise, perform the services and charge to the Contractor any cost incurred by the Government that is directly related to the performance of such service; or

(2) Terminate the contract for default.

(End of clause)

ATF-01 ACCESSIBILITY OF ELECTRONIC AND INFORMATION TECHNOLOGY (SECTION 508)

ACCESSIBILITY OF ELECTRONIC AND INFORMATION TECHNOLOGY (SECTION 508). *(Revised September 24, 2008)*

(a) Each Electronic and Information Technology (EIT) product furnished under this contract shall meet or exceed the Electronic and Information Technology Accessibility Standards (36 CFR 1194). If the Contracting Officer determines any furnished product is not in compliance with the Standards, the Contracting Officer will promptly inform the Contractor in writing. The Contractor shall, without charge to the Government, replace the non-compliant products within the period of time specified by the Government in writing. If such replacement is not completed within the time specified, the Government shall have the following recourses:

(1) cancellation of the contract, delivery or task order, purchase or line item without termination liabilities; or

(2) in the case of custom Electronic and Information Technology (EIT) being developed for the Government, the Government shall have the right to make any necessary changes or repairs itself or have another firm make the changes or repairs. The contractor shall reimburse the Government for any expenses incurred thereby.

(b) For every EIT product supplied under this contract that does not comply with 36 CFR 1194, the contractor shall make every effort to replace or upgrade with a compliant, equivalent product, if commercially available and cost neutral. The replacement will occur on either the planned refresh cycle of the product, or on the contract renewal date, whichever occurs first.

(End of Clause)

ATF-03 SECTION 508 TECHNICAL REQUIREMENTS

SECTION 508 TECHNICAL REQUIREMENTS. *(Revised September 24, 2008)*

Rehabilitation Act of 1973, Section 508 IT Accessibility Requirements

A. General

1. Purpose (Reference 36 CFR 1194.1)

(a)The below technical standards are those issued by the Architectural and Transportation Barriers Compliance Board (Access Board), pursuant to Section 508 (a) (2) (A) of the Rehabilitation Act Amendments of 1998 (29 U.S.C. 794 (d)) as enacted in the Workforce Investment Act of 1998.(The Access Board is an independent Federal agency established by Section 502 of the Rehabilitation Act (29 U.S.C. 792) whose primary mission is to promote accessibility for individuals with disabilities.)

(b)Section 508 requires that when Federal agencies develop, procure, maintain, or use electronic and information technology, Federal employees with disabilities have access to and use of information and data that is comparable to the access and use by Federal employees who are not individuals with disabilities, unless an undue burden would be imposed on the agency. Section 508 also requires that individuals with disabilities, who are members of the public seeking information or services from a Federal agency, have access to and use of information and data that is comparable to that provided to the public who are not individuals with disabilities, unless an undue burden would be imposed on the agency.

2. Application (Reference 36 CFR 1194.2)

(a)This section does not apply to Electronic and Information Technology (EIT, see definitions at A. 4. below) that is acquired by the contractor incidental to the contract, or is neither used nor accessed by Federal employees or members of the public, and contractor employees in their professional capacity are not considered members of the public.

(b)For any EIT product proposed in response to this solicitation as a deliverable that is a commercial item (as defined by the Federal Acquisition Regulation, Subpart 2.101) or any EIT product to be developed in response to this solicitation, that will be available to meet this contract's delivery requirements, the contractor must represent within his proposal that the product(s) complies with all of the below standards. The contractor must fully complete the spreadsheet, Electronic & Information Technology Accessibility Standards Evaluation, located as an attachment in Section J of this solicitation, and submit it with his/her proposal.

(c)If such product does not comply with all of the below standards, the contractor must specify each specific standard that is not met.

3. Electronic and Information Technology (EIT) Product General Exceptions (Reference 36 CFR 1194.3)

(a)This section does not apply to any EIT operated by agencies, the function, operation, or use of which involves:

- (1)Intelligence activities
- (2)Cryptographic activities related to national security
- (3)Command and control of military forces
- (4)Equipment as an integral part of a weapon or weapon system
- (5)Systems critical to the direct fulfillment of military or intelligence missions

(b)Products acquired by a contractor incidental to a contract, or are neither used nor accessed by Federal employees or members of the public, and contractor employees and all personnel related to the contract are not considered members of the public;

(c)Products or components of products that would require a fundamental alteration in their nature.

(d)Products located in spaces frequented only by service personnel for maintenance, repair or occasional monitoring.

4. Definitions (Reference 36 CFR 1194.4)

The following definitions apply to this section:

Agency. Any Federal department or agency, including the United States Postal Service.

Alternate formats. Alternate formats usable by people with disabilities may include, but are not limited to, Braille, ASCII text, large print, recorded audio, and electronic formats that comply with this part.

Alternate methods. Different means of providing information, including product documentation, to people with disabilities. Alternate methods may include, but are not limited to, voice, fax, relay service, TTY, Internet posting, captioning, text-to-speech synthesis, and audio description.

Assistive technology. Any item, piece of equipment, or system, whether acquired commercially, modified, or customized, that is commonly used to increase, maintain, or improve functional capabilities of individuals with disabilities.

Electronic and information technology. Includes information technology and any equipment or interconnected system or subsystem of equipment, that is used in the creation, conversion, or duplication of data or information. The term electronic and information technology includes, but is not limited to, telecommunications products (such as telephones), information kiosks and transaction machines, World Wide Web sites, multimedia, and office equipment such as copiers and fax machines. The term does not include any equipment that contains embedded information technology that is used as an integral part of the product, but the principal function of which is not the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. For example, HVAC (heating, ventilation, and air conditioning) equipment such as thermostats or temperature control devices, and medical equipment where information technology is integral to its operation, are not information technology.

Information technology. Any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

Operable controls. A component of a product that requires physical contact for normal operation. Operable controls include, but are not limited to, mechanically operated controls, input and output trays, card slots, keyboards, or keypads.

Product. Electronic and information technology.

Self Contained, Closed Products. Products that generally have embedded software and are commonly designed in such a fashion that a user cannot easily attach or install assistive technology. These products include, but are not limited to, information kiosks and information transaction machines, copiers, printers, calculators, fax machines, and other similar types of products.

Telecommunications. The transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received.

TTY. An abbreviation for teletypewriter. Machinery or equipment that employs interactive text based communications through the transmission of coded signals across the telephone network. TTYs may include, for example, devices known as TDDs (telecommunication display devices or telecommunication devices for deaf persons) or computers with special modems. TTYs are also called text telephones.

Undue burden. Undue burden means significant difficulty or expense. In determining whether an action would result in an undue burden, an agency shall consider all agency resources available to the program or component for which the product is being developed, procured, maintained, or used.

5. Equivalent Facilitation (Reference 36 CFR 1194.5)

Nothing in this part is intended to prevent the use of designs or technologies as alternatives to those prescribed in this part provided they result in substantially equivalent or greater access to and use of a product for people with disabilities.

B. Technical Standards

1194.21 Software applications and operating systems.

(a) When software is designed to run on a system that has a keyboard, product functions shall be executable from a keyboard where the function itself or the result of performing a function can be discerned textually.

(b) Applications shall not disrupt or disable activated features of other products that are identified as accessibility features, where those features are developed and documented according to industry standards. Applications also shall not disrupt or disable activated features of any operating system that are identified as accessibility features where the application programming interface for those accessibility features has been documented by the manufacturer of the operating system and is available to the product developer.

(c) A well-defined on-screen indication of the current focus shall be provided that moves among interactive interface elements as the input focus changes. The focus shall be programmatically exposed so that assistive technology can track focus and focus changes.

- (d)Sufficient information about a user interface element including the identity, operation and state of the element shall be available to assistive technology. When an image represents a program element, the information conveyed by the image must also be available in text.
- (e)When bitmap images are used to identify controls, status indicators, or other programmatic elements, the meaning assigned to those images shall be consistent throughout an application's performance.
- (f)Textual information shall be provided through operating system functions for displaying text. The minimum information that shall be made available is text content, text input caret location, and text attributes.
- (g)Applications shall not override user selected contrast and color selections and other individual display attributes.
- (h)When animation is displayed, the information shall be displayable in at least one non-animated presentation mode at the option of the user.
- (i)Color coding shall not be used as the only means of conveying information, indicating an action, prompting a response, or distinguishing a visual element.
- (j)When a product permits a user to adjust color and contrast settings, a variety of color selections capable of producing a range of contrast levels shall be provided.
- (k)Software shall not use flashing or blinking text, objects, or other elements having a flash or blink frequency greater than 2 Hz and lower than 55 Hz.
- (l)When electronic forms are used, the form shall allow people using assistive technology to access the information, field elements, and functionality required for completion and submission of the form, including all directions and cues.

1194.22 Web-based intranet and internet information and applications.

- (a)A text equivalent for every non-text element shall be provided (e.g., via "alt", "longdesc", or in element content).
- (b)Equivalent alternatives for any multimedia presentation shall be synchronized with the presentation.
- (c)Web pages shall be designed so that all information conveyed with color is also available without color, for example from context or markup.
- (d)Documents shall be organized so they are readable without requiring an associated style sheet.
- (e)Redundant text links shall be provided for each active region of a server-side image map.
- (f)Client-side image maps shall be provided instead of server-side image maps except where the regions cannot be defined with an available geometric shape.
- (g)Row and column headers shall be identified for data tables.
- (h)Frames shall be titled with text that facilitates frame identification and navigation.
- (i)Pages shall be designed to avoid causing the screen to flicker with a frequency greater than 2 Hz and lower than 55 Hz.
- (j)A text-only page, with equivalent information or functionality, shall be provided to make a web site comply with the provisions of this part, when compliance cannot be accomplished in any other way. The content of the text-only page shall be updated whenever the primary page changes.
- (k)When pages utilize scripting languages to display content, or to create interface elements, the information provided by the script shall be identified with functional text that can be read by assistive technology.
- (l)When a web page requires that an applet, plug-in or other application be present on the client system to interpret page content, the page must provide a link to a plug-in or applet that complies with1194.21(a) through (l).

(m)When electronic forms are designed to be completed on-line, the form shall allow people using assistive technology to access the information, field elements, and functionality required for completion and submission of the form, including all directions and cues.

(n)A method shall be provided that permits users to skip repetitive navigation links.

(o)When a timed response is required, the user shall be alerted and given sufficient time to indicate more time is required.

Note to 1. The Board interprets paragraphs (a) through (k) of this section as consistent with the following priority 1 Checkpoints of the Web Content Accessibility Guidelines 1.0 (WCAG 1.0) (May 5, 1999) published by the Web Accessibility Initiative of the World Wide Web Consortium:

Section 1194.22 Paragraph (a) WCAG 1.0 Checkpoint 1.1
 Section 1194.22 Paragraph (b) WCAG 1.0 Checkpoint 1.4
 Section 1194.22 Paragraph (c) WCAG 1.0 Checkpoint 2.1
 Section 1194.22 Paragraph (d) WCAG 1.0 Checkpoint 6.1
 Section 1194.22 Paragraph (e) WCAG 1.0 Checkpoint 1.2
 Section 1194.22 Paragraph (f) WCAG 1.0 Checkpoint 9.1
 Section 1194.22 Paragraph (g) WCAG 1.0 Checkpoint 5.1
 Section 1194.22 Paragraph (h) WCAG 1.0 Checkpoint 5.2
 Section 1194.22 Paragraph (i) WCAG 1.0 Checkpoint 12.1
 Section 1194.22 Paragraph (j) WCAG 1.0 Checkpoint 7.1
 Section 1194.22 Paragraph (k) WCAG 1.0 Checkpoint 11.4

2.Paragraphs (l), (m), (n), (o), and (p) of this section are different from WCAG 1.0. Web pages that conform to WCAG 1.0, level A (i.e., all priority 1 checkpoints) must also meet paragraphs (l), (m), (n), (o), and (p) of this section to comply with this section. WCAG 1.0 is available at <http://www.w3.org/TR/1999/WAI-WEBCONTENT-19990505>.

1194.23 Telecommunications products.

(a)Telecommunications products or systems which provide a function allowing voice communication and which do not themselves provide a TTY functionality shall provide a standard non-acoustic connection point for TTYs. Microphones shall be capable of being turned on and off to allow the user to intermix speech with TTY use.

(b)Telecommunications products which include voice communication functionality shall support all commonly used cross-manufacturer non-proprietary standard TTY signal protocols.

(c)Voice mail, auto-attendant, and interactive voice response telecommunications systems shall be usable by TTY users with their TTYs.

(d)Voice mail, messaging, auto-attendant, and interactive voice response telecommunications systems that require a response from a user within a time interval, shall give an alert when the time interval is about to run out, and shall provide sufficient time for the user to indicate more time is required.

(e)Where provided, caller identification and similar telecommunications functions shall also be available for users of TTYs, and for users who cannot see displays.

(f)For transmitted voice signals, telecommunications products shall provide a gain adjustable up to a minimum of 20 dB. For incremental volume control, at least one intermediate step of 12 dB of gain shall be provided.

(g)If the telecommunications product allows a user to adjust the receive volume, a function shall be provided to automatically reset the volume to the default level after every use.

(h)Where a telecommunications product delivers output by an audio transducer which is normally held up to the ear, a means for effective magnetic wireless coupling to hearing technologies shall be provided.

(i)Interference to hearing technologies (including hearing aids, cochlear implants, and assistive listening devices) shall be reduced to the lowest possible level that allows a user of hearing technologies to utilize the telecommunications product.

(j)Products that transmit or conduct information or communication, shall pass through cross-manufacturer, non-proprietary, industry-standard codes, translation protocols, formats or other information necessary to provide the information or communication in a

usable format. Technologies which use encoding, signal compression, format transformation, or similar techniques shall not remove information needed for access or shall restore it upon delivery.

(k) Products which have mechanically operated controls or keys, shall comply with the following:

- (1) Controls and keys shall be tactilely discernible without activating the controls or keys.
- (2) Controls and keys shall be operable with one hand and shall not require tight grasping, pinching, or twisting of the wrist. The force required to activate controls and keys shall be 5 lbs. (22.2 N) maximum.
- (3) If key repeat is supported, the delay before repeat shall be adjustable to at least 2 seconds. Key repeat rate shall be adjustable to 2 seconds per character.
- (4) The status of all locking or toggle controls or keys shall be visually discernible, and discernible either through touch or sound.

1194.24 Video and multimedia products.

(a) All analog television displays 13 inches and larger, and computer equipment that includes analog television receiver or display circuitry, shall be equipped with caption decoder circuitry which appropriately receives, decodes, and displays closed captions from broadcast, cable, videotape, and DVD signals. As soon as practicable, but not later than July 1, 2002, widescreen digital television (DTV) displays measuring at least 7.8 inches vertically, DTV sets with conventional displays measuring at least 13 inches vertically, and stand-alone DTV tuners, whether or not they are marketed with display screens, and computer equipment that includes DTV receiver or display circuitry, shall be equipped with caption decoder circuitry which appropriately receives, decodes, and displays closed captions from broadcast, cable, videotape, and DVD signals.

(b) Television tuners, including tuner cards for use in computers, shall be equipped with secondary audio program playback circuitry.

(c) All training and informational video and multimedia productions which support the agency's mission, regardless of format, that contain speech or other audio information necessary for the comprehension of the content, shall be open or closed captioned.

(d) All training and informational video and multimedia productions which support the agency's mission, regardless of format, that contain visual information necessary for the comprehension of the content, shall be audio described.

(e) Display or presentation of alternate text presentation or audio descriptions shall be user-selectable unless permanent.

1194.25 Self contained, closed products.

(a) Self contained products shall be usable by people with disabilities without requiring an end-user to attach assistive technology to the product. Personal headsets for private listening are not assistive technology.

(b) When a timed response is required, the user shall be alerted and given sufficient time to indicate more time is required.

(c) Where a product utilizes touch-screens or contact-sensitive controls, an input method shall be provided that complies with 1194.23

(k) (1) through (4).

(d) When biometric forms of user identification or control are used, an alternative form of identification or activation, which does not require the user to possess particular biological characteristics, shall also be provided.

(e) When products provide auditory output, the audio signal shall be provided at a standard signal level through an industry standard connector that will allow for private listening. The product must provide the ability to interrupt, pause, and restart the audio at anytime.

(f) When products deliver voice output in a public area, incremental volume control shall be provided with output amplification up to a level of at least 65 dB. Where the ambient noise level of the environment is above 45 dB, a volume gain of at least 20 dB above the ambient level shall be user selectable. A function shall be provided to automatically reset the volume to the default level after every use.

(g) Color coding shall not be used as the only means of conveying information, indicating an action, prompting a response, or distinguishing a visual element.

(h)When a product permits a user to adjust color and contrast settings, a range of color selections capable of producing a variety of contrast levels shall be provided.

(i)Products shall be designed to avoid causing the screen to flicker with a frequency greater than 2 Hz and lower than 55 Hz.

(j)Products which are freestanding, non-portable, and intended to be used in one location and which have operable controls shall comply with the following:

(1) The position of any operable control shall be determined with respect to a vertical plane, which is 48 inches in length, centered on the operable control, and at the maximum protrusion of the product within the 48 inch length (see Figure 1 of this part).

(2) Where any operable control is 10 inches or less behind the reference plane, the height shall be 54 inches maximum and 15 inches minimum above the floor.

(3) Where any operable control is more than 10 inches and not more than 24 inches behind the reference plane, the height shall be 46 inches maximum and 15 inches minimum above the floor.

(4) Operable controls shall not be more than 24 inches behind the reference plane (see Figure 2 of this part).

1194.26 Desktop and portable computers.

(a)All mechanically operated controls and keys shall comply with 1194.23 (k) (1) through (4).

(b)If a product utilizes touch-screens or touch-operated controls, an input method shall be provided that complies with 1194.23 (k) (1) through (4).

(c)When biometric forms of user identification or control are used, an alternative form of identification or activation, which does not require the user to possess particular biological characteristics, shall also be provided.

(d)Where provided, at least one of each type of expansion slots, ports and connectors shall comply with publicly available industry standards.

C. Functional Performance Criteria

1194.31 Functional performance criteria.

(a)At least one mode of operation and information retrieval that does not require user vision shall be provided, or support for assistive technology used by people who are blind or visually impaired shall be provided.

(b)At least one mode of operation and information retrieval that does not require visual acuity greater than 20/70 shall be provided in audio and enlarged print output working together or independently, or support for assistive technology used by people who are visually impaired shall be provided.

(c)At least one mode of operation and information retrieval that does not require user hearing shall be provided, or support for assistive technology used by people who are deaf or hard of hearing shall be provided.

(d)Where audio information is important for the use of a product, at least one mode of operation and information retrieval shall be provided in an enhanced auditory fashion, or support for assistive hearing devices shall be provided.

(e)At least one mode of operation and information retrieval that does not require user speech shall be provided, or support for assistive technology used by people with disabilities shall be provided.

(f)At least one mode of operation and information retrieval that does not require fine motor control or simultaneous actions and that is operable with limited reach and strength shall be provided.

D. Information, Documentation, and Support

1194.41 Information, documentation, and support.

(a)Product support documentation provided to end-users shall be made available in alternate formats upon request, at no additional charge.

(b)End-users shall have access to a description of the accessibility and compatibility features of products in alternate formats or alternate methods upon request, at no additional charge.

(c)Support services for products shall accommodate the communication needs of end-users with disabilities.

(End of Clause)

ATF-12 NON-US CITIZENS PROHIBITED FROM ACCESS TO DOJ INFORMATION TECHNOLOGY (IT) SYSTEMS

NON-US CITIZENS PROHIBITED FROM ACCESS TO DOJ INFORMATION TECHNOLOGY (IT) SYSTEMS. *(Revised May 31,2007)*

The Department of Justice does not permit the use of Non-U.S. citizens in the performance of this contract or commitment for any position that involves access to or development of any DOJ Information Technology (IT) system.By signing the contract or commitment document, the contractor agrees to this restriction.

In those instances where other non-IT requirements contained in the contract or commitment can be met by using Non-U.S. citizens, those requirements shall be clearly described.

Financial Responsibility: Contractor employees who have delinquent unpaid debt may be required to provide proof of payment and/or proof of participation in a payment plan. If this documentation cannot be provided, the Contractor employee's background investigation may be terminated and/or access to A TF facilities, proprietary information and data, including automated information systems, without being offered an opportunity to mitigate the information.

A contractor employee who is in direct violation of a policy established, by DOJ or ATF may be denied access to ATF facilities, proprietary information and data. including automated information systems, without being offered an opportunity to mitigate the information.

(End of Clause)

ATF-14 ELECTRONIC INVOICING

ELECTRONIC INVOICING *(Revised October 27,2008)*

The Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) encourages contractors to invoice electronically. Invoicing electronically saves time, money, and physical storage space for both the Government and the contractor.

Each invoice must be a proper invoice in accordance with Federal Acquisition Regulations (FAR) 32.905(b). The contractor may submit a combined invoice with each ATF contract/order number. The invoice must clearly identify the specific Contract Line Item (CLIN) or item number for which the contractor is seeking payment under the contract/order. If the invoice covers multiple CLINs or item numbers, the invoice must clearly identify specific amounts and activity applicable to each.

Electronic invoices must be submitted to the ATF Contracting Officer's Representative (COR)/POC named in Section G/Section 3.3 of this contract and Financial Management Division (FMD), Finance.Branch@ATF.gov. Electronic invoices will serve as the official original copy. The e-mail subject line must contain the name of the ATF COR/POC named in Section G/Section 3.3 of the obligation document, the Order/Award number, the Invoice number and Vendor name (*i.e.: John Doe_DJAXxxxxxxx_Invoice #xxx_ABC, Inc.*). ATF will return to the vendor any invoices that do not contain the correct subject line information.

Contractors who are unable to submit electronic invoices may mail their invoices to the COR/POC named in Section G/Section 3.3 of this contract and FMD address provided below:

Bureau of Alcohol, Tobacco, Firearms & Explosives
Attn: Finance Branch EXPEDITE CONTRACT INVOICE
99 New York Avenue, NE
Mail Drop 4S-288

Washington, DC 20226

(End of Clause)

ATF-17 NOTICE TO THE GOVERNMENT OF DELAYS

NOTICE TO THE GOVERNMENT OF DELAYS *(Revised July 19, 2007)*

In the event the Contractor encounters difficulty in meeting performance requirements, or when he anticipates difficulty in complying with the contract delivery schedule or completion date, or whenever the Contractor has knowledge that any actual or potential situation is delaying or threatens to delay the timely performance of the contract, the Contractor shall immediately notify the Contracting Officer and the Contracting Officer's Representative COR(s), in writing, giving pertinent details; provided, however, that this date shall be information only in character and that this provision shall not be construed as a waiver by the Government of any delivery schedule or date, or any rights or remedies provided by law or under this contract.

(End of Clause)

ATF-18 REQUIREMENTS FOR ACCESS TO LAW ENFORCEMENT SENSITIVE INFORMATION

REQUIREMENTS FOR ACCESS TO LAW-ENFORCEMENT SENSITIVE INFORMATION *(Revised July 19, 2007)*

(a) Duplication or disclosure of the data and other information to which the Contractor will have access as a result of this contract is prohibited. It is understood that throughout performance of this contract, the Contractor will have access to confidential and sensitive data, which is either the sole property of the Government or is the sole property of other than the contracting parties. The Contractor and its subcontractor(s) *(if any)* agree to maintain the confidentiality of all data to which access may be gained throughout the contract performance, whether title thereto vests in the Government or otherwise. The Contractor and its subcontractor(s) *(if any)* agree to not disclose said data, any interpretations and/or translations thereof, or data derivatives, to unauthorized parties in contravention of these provisions, without the prior written approval of the Contracting Officer or the party in which title thereto is wholly vested. Subcontractors are subject to the same stipulations and may be held responsible for any violations of confidentiality.

(b) The Contractor agrees that each Contractor employee, prior to and as a pre-condition for employment relating to the subject matter of this order, will be required to execute a Nondisclosure Agreement as provided. The Contractor shall provide the Contracting Officer with the original copy of this form signed by each employee prior to the employee's start date on the contract.

(End of Clause)

ATF-19 AUTHORITY TO OBLIGATE THE GOVERNMENT

AUTHORITY TO OBLIGATE THE GOVERNMENT *(Revised July 19, 2007)*

The Contracting Officer is the only individual who can legally commit or obligate the Government to the expenditure of public funds. No cost chargeable to the proposed contract can be incurred before receipt of a fully executed contract or specific authorization from the Contracting Officer.

(End of Clause)

ATF-21 ALL ITEMS TO BECOME THE PROPERTY OF THE GOVERNMENT

ALL ITEMS TO BECOME THE PROPERTY OF THE GOVERNMENT *(Revised July 19, 2007)*

Title to all source data and materials furnished by the Government, together with all plans, designs, reports, materials, programs and documentation thereof and all other items pertaining to the work and services to be performed under orders pursuant to this contract

shall become and remain with the Government upon completion. The Government shall have the full right to use each of these for its purposes without compensation or approval on the part of the Contractor. The Government shall have access to and the right to make copies of the above mentioned items. All proprietary information, programs, etc. shall be indicated as such in the Contractor's proposal. The identification of information, programs, etc. as proprietary or confidential is for information purposes only and shall not be binding on the Government to prevent disclosure of such information. The offeror is advised that such information may be subject to release upon request pursuant to the Freedom of Information Act (5 U.S.C. 552).

(End of Clause)

ATF-22 CONFIDENTIALITY OF INFORMATION AND DISCLOSURE

CONFIDENTIALITY OF INFORMATION AND DISCLOSURE *(Revised April 3, 2008)*

The Contractor agrees, in the performance of this contract, to keep all information contained in source documents or other media furnished by the Government in the strictest confidence. The Contractor also agrees not to publish or otherwise divulge such information in whole or in part, in any manner or form, nor to authorize or permit others to do so, taking such reasonable measures as are necessary to restrict access to such information while in the Contractor's possession, to those employees needing such information to perform the work provided herein, e.g., on a need to know basis. There shall be no dissemination or publication, except within and between the Contractor and any subcontractors, of information developed under this contract or contained in the reports to be furnished pursuant to this contract without prior written approval from the Contracting Officer. No news release (including photographs and films, public announcements, denial or confirmation of same) on any part of the subject matter of this contract or any phase of any program hereunder shall be made without the prior written approval of the Contracting Officer. The Contractor is prohibited from releasing to any source, other than the sponsoring activity, any interim, draft and final reports or information pertaining to services performed under this contract until report approval or official review has been obtained. Furthermore, the contractor shall insure that the cover of all interim, draft and final reports contain the following statement: "The view, opinions, and/or findings contained in this report are those of the author(s) and should not be construed as an official Government position, policy or decision, unless so designated by other documentation."

The Contractor agrees to immediately notify in writing the Contracting Officer named herein, in the event that the Contractor determines or has reason to suspect a breach of this requirement. The Contractor agrees to insert the substance of this clause in any consultant agreement or subcontract hereunder.

(a) Confidential information, as used in this clause, means (1) information or data of a personal nature proprietary about an individual, or (2) information or data submitted by or pertaining CONFIDENTIALITY to an institution or organization, or (3) information or data pertaining to a law enforcement investigation or operation.

(b) In addition to the types of confidential information described in (a) (1), (2) and (3) above, information which might require special consideration with regard to the timing of its disclosure such as draft budget and strategic plans, studies or research, audits, etc.

(c) The Contracting Officer and the Contractor may, by mutual consent, identify elsewhere in this contract specific information and/or categories of information which the Government will furnish to the Contractor or that the Contractor is expected to generate which is confidential. Similarly, the Contracting Officer and the Contractor may, by mutual consent, identify such confidential information from time to time during the performance of the contract. Failure to agree will be settled pursuant to the Disputes clause.

(d) If it is established that information to be utilized under this contract is subject to the Privacy Act, the Contractor will follow the rules and procedures of the disclosure set forth in the Privacy Act of 1974, 5 U.S.C. 552a, and implementing regulations and policies, with respect to systems of records determined to be subject to the Privacy Act.

(e) Confidential information, as defined in (a)(1) and (2) above, shall not be disclosed without the prior written consent of the individual, institution, or organization. Confidential information, as defined in (a)(3) shall not be disclosed without the prior written consent of the Bureau of Alcohol, Tobacco, Firearms & Explosives (ATF).

(f) Whenever the Contractor is uncertain with regard to the proper handling of material under the contract, or if the material in question is subject to the Privacy Act or is confidential information subject to the provisions of this clause, the Contractor shall obtain a written determination from the Contracting Officer prior to any release, disclosure, dissemination, or publication.

(g) The provisions of paragraph (e) of this clause shall not apply when the information is subject to conflicting or overlapping provisions in other Federal, State, or local laws.

(End of Clause)

ATF-23 PRIVACY OR SECURITY SAFEGUARDS

PRIVACY OR SECURITY SAFEGUARDS *(August 1, 2007)*

(a) The details of any and all safeguards that the Contractor may design or develop under this contract shall become and shall remain the property of the Government and shall not be published or disclosed in any manner without the expressed written consent of the Government.

(b) The details of any and all safeguards that may be revealed to the Contractor by the Government in the course of performing under this contract shall not be published or disclosed in any manner without the expressed written consent of the Government.

(c) The Government shall be afforded full, free, and uninhibited access to all facilities, installations, technical capabilities, operations, documentation, records, and databases for the purpose of carrying out a program of inspection to ensure continued efficiency and efficacy of safeguards against threats and hazards to data security, integrity, and confidentiality.

(d) If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party. Mutual agreement shall then be reached on changes or corrections to existing safeguards or institution of new safeguards, with final determination or appropriateness being made by the Government. The Government's liability is limited to an equitable adjustment of cost for such changes or corrections, and the Government shall not be liable for claims of loss of business, damage to reputation, or damages of any other kind arising from discovery of new or unanticipated threats or hazards, or any public or private disclosure thereof.

(End of Clause)

ATF-24 COMPUTER SECURITY

COMPUTER SECURITY *(Revised August 17, 2010)*

(a) The Contractor is responsible for briefing their staff on accountability, system security requirements and sound security practices. All contractors will be briefed by the Contracting Officer's Representative (COR) on and must comply with US Department of Justice and ATF's Information Systems Security Directives. Each contractor assigned under this contract are required to sign the Certification Statements, indicating the individual has read and will comply with the order or directives.

(b) The Contractor will ensure that all departing contractor employees turn in their identification cards, keys, programs, data files, etc. within their possession. The Contractor will certify to the Contracting officer that the hard disk drives of any workstations and/or laptops used by their departing employees have been purged of all Government information, unless such equipment is reassigned to another employee on this contract. Additionally, the COR will notify the Information Services Division Operations Systems Branch when a contractor is departing so that his/her access can be removed from all information systems accesses that they were assigned as a user.

(c) At the termination of this contract, the Contractor shall certify in writing that all Government information has been cleared and purged from all contractor-owned equipment and electronic storage media. Government information on electronic media includes any data remanence from temporary file storage during processing.

(d) If system development, maintenance, or enhancements are performed as part of this contract, the Contractor will comply with ATF Information Systems Security Office policy and procedures to ensure the work being performed meets the minimum-security requirements. Contact the Information Systems Security Office at 202-648-9510, for the current policy and procedures.

COMPUTER SECURITY TRAINING

All contractor employees must complete operations security training, presented by ATF, after contract award. The time and location of this training will be scheduled by ATF. Computer Security Awareness Training, presented by ATF, shall be completed on a yearly basis.

ATF reserves the right to limit or deny access of contractor employees to ATF information, services or systems in the event of a breach of this clause, or of any ATF, Department of Justice or other applicable law, regulation or policy.

(End of Clause)

ATF-27 INFORMATION RESELLERS OR DATA BROKERS

INFORMATION RESELLERS OR DATA BROKERS *(Revised July 24, 2008)*

Under this contract, the Department obtains personally identifiable information about individuals from the contractor. The contractor hereby certifies that it has a security policy in place which contains procedures to promptly notify any individual whose personally identifiable information (as defined by the Office of Management and Budget) was, or is reasonably believed to have been, lost or acquired by an unauthorized person while the data is under the control of the contractor. In any case in which the data that was lost or improperly acquired reflects or consists of data that originated within the Department, or reflects sensitive law enforcement or national security interest in the data, the contractor shall notify the ATF contracting officer so that ATF may determine whether notification would impede a law enforcement investigation or jeopardize national security. In such cases, the contractor shall not notify the individuals until it receives further instruction and approval from the ATF's Office of Science and Technology, Information Systems Security Office. The contractor assumes full responsibility for taking corrective action consistent with the Department's Data Breach Notification Procedures, which may include offering credit monitoring when appropriate.

(End of Clause)

ATF-28 CONTRACTOR CERTIFICATION OF COMPLIANCE WITH FEDERAL TAX REQUIREMENTS

CONTRACTOR CERTIFICATION OF COMPLIANCE WITH FEDERAL TAX REQUIREMENTS *(Revised May 22, 2008)*

By submitting a response to a solicitation or accepting a contract award, the contractor certifies that, to the best of its knowledge and belief, the contractor has filed all Federal tax returns required during the three years preceding the certification, has not been convicted of a criminal offense under the Internal Revenue Code of 1986, and has not, more than 90 days prior to certification, been notified of any unpaid Federal tax assessment for which the liability remains unsatisfied, unless the assessment is the subject of an installment agreement or offer in compromise that has been approved by the Internal Revenue Service and is not in default, or the assessment is the subject of a nonfrivolous administrative or judicial proceeding.

(End of Clause)

ATF-30 COMMON SECURITY CONFIGURATIONS

COMMON SECURITY CONFIGURATIONS *(from PGD 11-08 dated April 11, 2011)*

(a) The provider of information technology shall certify applications are fully functional and operate correctly as intended on systems using the Federal Desktop Core Configuration (FDCC) or the United States Government Configuration Baseline (USGCB). This includes Internet Explorer 7 and 8 configured to operate on Windows XP, Windows

Vista and Windows 7 (in Protected Mode on Windows Vista and Windows 7). For the Windows XP settings, see http://csrc.nist.gov/itsec/guidance_WinXP.html. For the Windows Vista settings, see http://csrc.nist.gov/itsec/guidance_vista.html. For Windows 7 settings, see http://usgcb.nist.gov/usgcb_content.html.

(b) The standard installation, operation, maintenance, update, and/or patching of software shall not alter the configuration settings from the approved FDCC or USGCB configuration. The information technology should also use the Windows Installer Service for installation to the default "program files" directory and should be able to silently install and uninstall.

(c) Applications designed for normal end users shall run in the standard user context without elevated system administration privileges.

(End of Clause)

ATF-35 52.232-99, Providing Accelerated Payment to Small Business Subcontractors (DEVIATION) (AUG 2012)

**52.232-99 - PROVIDING ACCELERATED PAYMENT TO
SMALL BUSINESS SUBCONTRACTORS
(DEVIATION) (AUG 2012)**

This clause implements the temporary policy provided by OMB Policy Memorandum M- 12-16, *Providing Prompt Payment to Small Business Subcontractors*, dated July 11, 2012.

(a) Upon receipt of accelerated payments from the Government, the contractor is required to make accelerated payments to small business subcontractors to the maximum extent practicable after receipt of a proper invoice and all proper documentation from the small business subcontractor.

(b) Include the substance of this clause, including this paragraph (b), in all subcontracts with small business concerns.

(c) The acceleration of payments under this clause does not provide any new rights under the Prompt Payment Act.

End of Clause

ATF-38 Representation Regarding Acquisition by Lease, Purchase or Otherwise of any Equipment or Software (November 2013)

Representation Regarding Acquisition by Lease, Purchase or Otherwise, of any Equipment or Software to be used in, on, or to support any Department IT System where such Equipment or Software is Produced, Manufactured or Assembled by One or More Entities Owned, Directed or Subsidized by China.

In accordance with sections Section 516 of the Department Fiscal Year 2013 (FY 2013) Appropriations Act (Consolidated and Further Continuing Appropriations Act of 2013, Division B, Public Law 113-6) no funds may be used to acquire equipment to be used in, on, or to support any Department IT system produced, manufactured or assembled by one or more entities owned, directed or subsidized by China *unless* an agency has determined that the acquisition is in the national interest of the United States.

Accordingly,

A. By accepting this award or order, in writing or by performance, the offeror/contractor represents that, as of the date of this award or order, either (mark the paragraph that applies):

[] No equipment to be used in, on, or to support any Department IT system in performance of the subject work is produced, manufactured, or assembled by one or more entities owned, directed or subsidized by China: or

[] One or more pieces of equipment to be used in, on, or to support any Department IT system in performance of the subject work is produced, manufactured, or assembled by one or more entities owned, directed or subsidized by China.

B. If the offeror represents that, as of the date of this award or order, any equipment to be used in, on, or to support any Department IT system in performance of the subject work is produced, manufactured, or assembled by one or more entities owned, directed or subsidized by China, the offer shall identify each such item and the vendor's /manufacturer's company name and address.

C. If the Department fails to approve in accordance with Section 516 of the Department's FY 2013 Appropriation Act, any piece of equipment that the offeror/contractor identifies in response to this clause, the Contracting Officer will so advise the offeror/contractor, and may provide the offeror/contractor with the opportunity to revise its offer.

(End of Clause)

ATF-41 DEPARTMENT POLICY ON DOMESTIC VIOLENCE, SEXUAL ASSAULT, AND STALKING

DEPARTMENT POLICY ON DOMESTIC VIOLENCE, SEXUAL ASSAULT, AND STALKING (July 2019)

It is the Department's policy to enhance workplace awareness of and safety for victims of domestic violence, sexual assault, and stalking. This policy is summarized in DOJ Policy Statement 1200.02 (Policy Statement), available in full for public viewing at:

<https://www.justice.gov/sites/default/files/ovw/legacy/2013/12/19/federal-workplace-responses-to-domesticviolence-sexualassault-stalking.pdf>

Vendor agrees, upon contract award, to provide notice of this Policy Statement, including at a minimum the above-listed URL, to all of Vendor's employees and employees of subcontractors who will be assigned to work on Department premises.

Upon contract award, the Department will notify contractor of the name and contract information for the Point of Contact for Victims of domestic violence, sexual assault, and stalking for the component or components where Contractor will be performing. The name and contact information for the ATF Contractor Victim Point of Contact (CV POC) is Mr. Kenneth Houser, Bureau Procurement Chief, (202) 648-7693. Contractor agrees to inform its employees and employees of subcontractors who will be assigned to work on Department premises of the name and contact information for the Victim Point of Contact.

(End of Clause)

ATF-46 Corporate Representation Regarding Felony Conviction Under Any Federal Law or Unpaid Delinquent Tax Liability - Award (DEVIATION 2015-02) (March 2015)

Corporate Representation Regarding Felony Conviction Under Any Federal Law or Unpaid Delinquent Tax Liability - Award (DEVIATION 2015-02) (March 2015)

(a) None of the funds made available by the Department's current Appropriations Act may be used to enter into a contract, memorandum of understanding, or cooperative agreement with a corporation –

(1) convicted of a felony criminal violation under any Federal law within the preceding 24 months, where the awarding agency is aware of the conviction, unless an agency has considered suspension or debarment of the corporation and made a determination that this further action is not necessary to protect the interests of the Government, or

(2) that has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability, where the awarding agency is aware of the unpaid tax liability, *unless* an agency has considered suspension or debarment of the corporation and made a determination that this further action is not necessary to protect the interests of the Government.

(b) By accepting this award or order, in writing or by performance, the offeror/contractor represents that –

(1) the offeror is not a corporation convicted of a felony criminal violation under any Federal or State law within the preceding 24 months; and,

(2) the offeror is *not* a corporation that has any unpaid Federal or State tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability.

(End of Clause)

ATF-47 Contractor Internal Confidentiality Agreements or Statements Prohibiting or Restricting Reporting of Waste, Fraud, and Abuse - Award (DEVIATION 2015-02) (March 2015)

Contractor Internal Confidentiality Agreements or Statements Prohibiting or Restricting Reporting of Waste, Fraud, and Abuse – Award (DEVIATION 2015-02) (March 2015)

By accepting this award or order, the contractor certifies that it does *not* require employees or contractors of the contractor seeking to report fraud, waste, and abuse to sign internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or contractors from lawfully reporting waste, fraud, and abuse to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information.

(End of Clause)

ATF-48 Contractor Certification of Compliance with Federal Tax Requirements - Award (DEVIATION 2015-02) (March 2015)

Contractor Certification of Compliance with Federal Tax Requirements – Award (DEVIATION 2015-02) (March 2015)

By accepting this award or order, the contractor certifies that, to the best of its knowledge and belief, the contractor has (a) filed all Federal tax returns required during the three years preceding the certification, (b) not been convicted of a criminal offense under the Internal Revenue Code of 1986, and (c) not been notified, more than 90 days before the subject certification, of any unpaid Federal tax assessment for which the liability remains unsatisfied, unless the assessment is the subject of an installment agreement or offer in compromise that has been approved by the Internal Revenue Service and is not in default, or the assessment is the subject of a non-frivolous administrative or judicial proceeding.

(End of Clause)

ATF-49 ATF-49 SECURITY OF INFORMATION AND INFORMATION SYSTEMS, INCLUDING PERSONALLY-IDENTIFIABLE DATA (PII) (Revised April 8, 2016)

I. Applicability to Contractors and Subcontractors

This clause applies to all contractors and subcontractors, including cloud service providers (“CSPs”), and personnel of contractors, subcontractors, and CSPs (hereinafter collectively, “Contractor”) that may access, collect, store, process, maintain, use, share, retrieve, disseminate, transmit, or dispose of DOJ Information. It establishes and implements specific DOJ requirements applicable to this Contract. The requirements established herein are in addition to those required by the Federal Acquisition Regulation (“FAR”), including FAR 11.002(g) and 52.239-1, the Privacy Act of 1974, and any other applicable laws, mandates, Procurement Guidance Documents, and Executive Orders pertaining to the development and operation of Information Systems and the protection of Government Information. This clause does not alter or diminish any existing rights, obligation or liability under any other civil and/or criminal law, rule, regulation or mandate.

II. General Definitions

The following general definitions apply to this clause. Specific definitions also apply as set forth in other paragraphs.

A. Information means any communication or representation of knowledge such as facts, data, or opinions, in any form or medium, including textual, numerical, graphic, cartographic, narrative, or audiovisual. Information includes information in an electronic format that allows it be stored, retrieved or transmitted, also referred to as “data,” and “personally identifiable information” (“PII”), regardless of form.

B. Personally Identifiable Information (or PII) means any information about an individual maintained by an agency, including, but not limited to, information related to education, financial transactions, medical history, and criminal or employment history and information, which can be used to distinguish or trace an individual's identity, such as his or her name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

C. DOJ Information means any Information that is owned, produced, controlled, protected by, or otherwise within the custody or responsibility of the DOJ, including, without limitation, Information related to DOJ programs or personnel. It includes, without limitation, Information

(1) provided by or generated for the DOJ, (2) managed or acquired by Contractor for the DOJ in connection with the performance of the contract, and/or (3) acquired in order to perform the contract.

D. Information System means any resources, or set of resources organized for accessing, collecting, storing, processing, maintaining, using, sharing, retrieving, disseminating, transmitting, or disposing of (hereinafter collectively, "processing, storing, or transmitting") Information.

E. Covered Information System means any information system used for, involved with, or allowing, the processing, storing, or transmitting of DOJ Information.

III. Confidentiality and Non-disclosure of DOJ Information

A. Preliminary and final deliverables and all associated working papers and material generated by Contractor containing DOJ Information are the property of the U.S. Government and must be submitted to the Contracting Officer ("CO") or the CO's Representative ("COR") at the conclusion of the contract. The U.S. Government has unlimited data rights to all such deliverables and associated working papers and materials in accordance with FAR 52.227-14.

B. All documents produced in the performance of this contract containing DOJ Information are the property of the U.S. Government and Contractor shall neither reproduce nor release to any third-party at any time, including during or at expiration or termination of the contract without the prior written permission of the CO.

C. Any DOJ information made available to Contractor under this contract shall be used only for the purpose of performance of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of this contract. In performance of this contract, Contractor assumes responsibility for the protection of the confidentiality of any and all DOJ Information processed, stored, or transmitted by the Contractor. When requested by the CO (typically no more than annually), Contractor shall provide a report to the CO identifying, to the best of Contractor's knowledge and belief, the type, amount, and level of sensitivity of the DOJ Information processed, stored, or transmitted under the Contract, including an estimate of the number of individuals for whom PII has been processed, stored or transmitted under the Contract and whether such information includes social security numbers (in whole or in part).

I. Applicability to Contractors and Subcontractors

This clause applies to all contractors and subcontractors, including cloud service providers ("CSPs"), and personnel of contractors, subcontractors, and CSPs (hereinafter collectively, "Contractor") that may access, collect, store, process, maintain, use, share, retrieve, disseminate, transmit, or dispose of DOJ Information. It establishes and implements specific DOJ requirements applicable to this Contract. The requirements established herein are in addition to those required by the Federal Acquisition Regulation ("FAR"), including FAR 11.002(g) and 52.239-1, the Privacy Act of 1974, and any other applicable laws, mandates, Procurement Guidance Documents, and Executive Orders pertaining to the development and operation of Information Systems and the protection of Government Information. This clause does not alter or diminish any existing rights, obligation or liability under any other civil and/or criminal law, rule, regulation or mandate.

II. General Definitions

The following general definitions apply to this clause. Specific definitions also apply as set forth in other paragraphs.

A. Information means any communication or representation of knowledge such as facts, data, or opinions, in any form or medium, including textual, numerical, graphic, cartographic, narrative, or audiovisual. Information includes information in an electronic format that allows it be stored, retrieved or transmitted, also referred to as "data," and "personally identifiable information" ("PII"), regardless of form.

B. Personally Identifiable Information (or PII) means any information about an individual maintained by an agency, including, but not limited to, information related to education, financial transactions, medical history, and criminal or employment history and information, which can be used to distinguish or trace an individual's identity, such as his or her name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

C. DOJ Information means any Information that is owned, produced, controlled, protected by, or otherwise within the custody or responsibility of the DOJ, including, without limitation, Information related to DOJ programs or personnel. It includes, without limitation, Information

(1) provided by or generated for the DOJ, (2) managed or acquired by Contractor for the DOJ in connection with the performance of the contract, and/or (3) acquired in order to perform the contract.

D. Information System means any resources, or set of resources organized for accessing, collecting, storing, processing, maintaining, using, sharing, retrieving, disseminating, transmitting, or disposing of (hereinafter collectively, "processing, storing, or transmitting") Information.

E. Covered Information System means any information system used for, involved with, or allowing, the processing, storing, or transmitting of DOJ Information.

III. Confidentiality and Non-disclosure of DOJ Information

A. Preliminary and final deliverables and all associated working papers and material generated by Contractor containing DOJ Information are the property of the U.S. Government and must be submitted to the Contracting Officer ("CO") or the CO's Representative ("COR") at the conclusion of the contract. The U.S. Government has unlimited data rights to all such deliverables and associated working papers and materials in accordance with FAR 52.227-14.

B. All documents produced in the performance of this contract containing DOJ Information are the property of the U.S. Government and Contractor shall neither reproduce nor release to any third-party at any time, including during or at expiration or termination of the contract without the prior written permission of the CO.

C. Any DOJ information made available to Contractor under this contract shall be used only for the purpose of performance of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of this contract. In performance of this contract, Contractor assumes responsibility for the protection of the confidentiality of any and all DOJ Information processed, stored, or transmitted by the Contractor.

When requested by the CO (typically no more than annually), Contractor shall provide a report to the CO identifying, to the best of Contractor's knowledge and belief, the type, amount, and level of sensitivity of the DOJ Information processed, stored, or transmitted under the Contract, including an estimate of the number of individuals for whom PII has been processed, stored or transmitted under the Contract and whether such information includes social security numbers (in whole or in part).

IV. Compliance with Information Technology Security Policies, Procedures and Requirements

A. For all Covered Information Systems, Contractor shall comply with all security requirements, including but not limited to the regulations and guidance found in the Federal Information Security Management Act of 2014 ("FISMA"), Privacy Act of 1974, E-Government Act of 2002, National Institute of Standards and Technology ("NIST") Special Publications ("SP"), including NIST SP 800-37, 800-53, and 800-60 Volumes I and II, Federal Information Processing Standards ("FIPS") Publications 140-2, 199, and 200, OMB Memoranda, Federal Risk and Authorization Management Program ("FedRAMP"), DOJ IT Security Standards, including DOJ Order 2640.2, as amended. These requirements include but are not limited to:

1. Limiting access to DOJ Information and Covered Information Systems to authorized users and to transactions and functions that authorized users are permitted to exercise;
2. Providing security awareness training including, but not limited to, recognizing and reporting potential indicators of insider threats to users and managers of DOJ Information and Covered Information Systems;
3. Creating, protecting, and retaining Covered Information System audit records, reports, and supporting documentation to enable reviewing, monitoring, analysis, investigation, reconstruction, and reporting of unlawful, unauthorized, or inappropriate activity related to such Covered Information Systems and/or DOJ Information;
4. Maintaining authorizations to operate any Covered Information System;
5. Performing continuous monitoring on all Covered Information Systems;
6. Establishing and maintaining baseline configurations and inventories of Covered Information Systems, including hardware, software, firmware, and documentation, throughout the Information System Development Lifecycle, and establishing and enforcing security configuration settings for IT products employed in Information Systems;
7. Ensuring appropriate contingency planning has been performed, including DOJ Information and Covered Information System backups;
8. Identifying Covered Information System users, processes acting on behalf of users, or

devices, and authenticating and verifying the identities of such users, processes, or devices, using multifactor authentication or HSPD-12 compliant authentication methods where required;

9. Establishing an operational incident handling capability for Covered Information Systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities, and tracking, documenting, and reporting incidents to appropriate officials and authorities within Contractor's organization and the DOJ;

10. Performing periodic and timely maintenance on Covered Information Systems, and providing effective controls on tools, techniques, mechanisms, and personnel used to conduct such maintenance;

12. Protecting Covered Information System media containing DOJ Information, including paper, digital and electronic media; limiting access to DOJ Information to authorized users; and sanitizing or destroying Covered Information System media containing DOJ Information before disposal, release or reuse of such media;

13. Limiting physical access to Covered Information Systems, equipment, and physical facilities housing such Covered Information Systems to authorized U.S. citizens unless a waiver has been granted by the Contracting Officer ("CO"), and protecting the physical facilities and support infrastructure for such Information Systems;

14. Screening individuals prior to authorizing access to Covered Information Systems to ensure compliance with DOJ Security standards;

15. Assessing the risk to DOJ Information in Covered Information Systems periodically, including scanning for vulnerabilities and remediating such vulnerabilities in accordance with DOJ policy and ensuring the timely removal of assets no longer supported by the Contractor;

16. Assessing the security controls of Covered Information Systems periodically to determine if the controls are effective in their application, developing and implementing plans of action designed to correct deficiencies and eliminate or reduce vulnerabilities in such Information Systems, and monitoring security controls on an ongoing basis to ensure the continued effectiveness of the controls;

17. Monitoring, controlling, and protecting information transmitted or received by Covered Information Systems at the external boundaries and key internal boundaries of such Information Systems, and employing architectural designs, software development techniques, and systems engineering principles that promote effective security; and

18. Identifying, reporting, and correcting Covered Information System security flaws in a timely manner, providing protection from malicious code at appropriate locations, monitoring security alerts and advisories and taking appropriate action in response.

B. Contractor shall not process, store, or transmit DOJ Information using a Covered Information System without first obtaining an Authority to Operate ("ATO") for each Covered Information System. The ATO shall be signed by the Authorizing Official for the DOJ component responsible for maintaining the security, confidentiality, integrity, and availability of the DOJ Information under this contract. The DOJ standards and requirements for obtaining an ATO may be found at DOJ Order 2640.2, as amended. (For Cloud Computing Systems, see Section V, below.)

C. Contractor shall ensure that no Non-U.S. citizen accesses or assists in the development, operation, management, or maintenance of any DOJ Information System, unless a waiver has been granted by the DOJ Component Head (or his or her designee) responsible for the DOJ Information System, the DOJ Chief Information Officer, and the DOJ Security Officer.

D. When requested by the DOJ CO or COR, or other DOJ official as described below, in connection with DOJ's efforts to ensure compliance with security requirements and to maintain and safeguard against threats and hazards to the security, confidentiality, integrity, and availability of DOJ Information, Contractor shall provide DOJ, including the Office of Inspector General ("OIG") and Federal law enforcement components, (1) access to any and all information and records, including electronic information, regarding a Covered Information System, and (2) physical access to Contractor's facilities, installations, systems, operations, documents, records, and databases. Such access may include independent validation testing of controls, system penetration testing, and FISMA data reviews by DOJ or agents acting on behalf of DOJ, and such access shall be provided within 72 hours of the request. Additionally, Contractor shall cooperate with DOJ's efforts to ensure, maintain, and safeguard the security, confidentiality, integrity, and availability of DOJ Information.

E. The use of Contractor-owned laptops or other portable digital or electronic media to process or store DOJ Information covered by this clause is prohibited until Contractor provides a letter to the DOJ CO, and obtains the CO's approval, certifying compliance with the following requirements:

1. Media must be encrypted using a NIST FIPS 140-2 approved product;
 2. Contractor must develop and implement a process to ensure that security and other applications software is kept up-to-date;
 3. Where applicable, media must utilize antivirus software and a host-based firewall mechanism;
 4. Contractor must log all computer-readable data extracts from databases holding DOJ Information and verify that each extract including such data has been erased within 90 days of extraction or that its use is still required. All DOJ Information is sensitive information unless specifically designated as non-sensitive by the DOJ; and,
 5. A Rules of Behavior ("ROB") form must be signed by users. These rules must address, at a minimum, authorized and official use, prohibition against unauthorized users and use, and the protection of DOJ Information. The form also must notify the user that he or she has no reasonable expectation of privacy regarding any communications transmitted through or data stored on Contractor-owned laptops or other portable digital or electronic media.
- F. Contractor-owned removable media containing DOJ Information shall not be removed from DOJ facilities without prior approval of the DOJ CO or COR.
- G. When no longer needed, all media must be processed (sanitized, degaussed, or destroyed) in accordance with DOJ security requirements.
- H. Contractor must keep an accurate inventory of digital or electronic media used in the performance of DOJ contracts.
- I. Contractor must remove all DOJ Information from Contractor media and return all such information to the DOJ within 15 days of the expiration or termination of the contract, unless otherwise extended by the CO, or waived (in part or whole) by the CO, and all such information shall be returned to the DOJ in a format and form acceptable to the DOJ. The removal and return of all DOJ Information must be accomplished in accordance with DOJ IT Security Standard requirements, and an official of the Contractor shall provide a written certification certifying the removal and return of all such information to the CO within 15 days of the removal and return of all DOJ Information.
- J. DOJ, at its discretion, may suspend Contractor's access to any DOJ Information, or terminate the contract, when DOJ suspects that Contractor has failed to comply with any security requirement, or in the event of an Information System Security Incident (see Section V.E. below), where the Department determines that either event gives cause for such action. The suspension of access to DOJ Information may last until such time as DOJ, in its sole discretion, determines that the situation giving rise to such action has been corrected or no longer exists. Contractor understands that any suspension or termination in accordance with this provision shall be at no cost to the DOJ, and that upon request by the CO, Contractor must immediately return all DOJ Information to DOJ, as well as any media upon which DOJ Information resides, at Contractor's expense.
- V. Cloud Computing
- A. Cloud Computing means an Information System having the essential characteristics described in NIST SP 800-145, The NIST Definition of Cloud Computing. For the sake of this provision and clause, Cloud Computing includes Software as a Service, Platform as a Service, and Infrastructure as a Service, and deployment in a Private Cloud, Community Cloud, Public Cloud, or Hybrid Cloud.
- B. Contractor may not utilize the Cloud system of any CSP unless:
1. The Cloud system and CSP have been evaluated and approved by a 3PAO certified under FedRAMP and Contractor has provided the most current Security Assessment Report ("SAR") to the DOJ CO for consideration as part of Contractor's overall System Security Plan, and any subsequent SARs within 30 days of issuance, and has received an ATO from the Authorizing Official for the DOJ component responsible for maintaining the security confidentiality, integrity, and availability of the DOJ Information under contract; or,
 2. If not certified under FedRAMP, the Cloud System and CSP have received an ATO signed by the Authorizing Official for the DOJ component responsible for maintaining the security, confidentiality, integrity, and availability of the DOJ Information under the contract.
- C. Contractor must ensure that the CSP allows DOJ to access and retrieve any DOJ Information processed, stored or transmitted in a Cloud system under this Contract within a reasonable time of any such request, but in no event less than 48 hours from the request. To ensure that the DOJ can fully and appropriately search and retrieve DOJ Information from the Cloud system, access shall include any schemas, meta-data, and other associated data artifacts.
- VI. Information System Security Breach or Incident
- A. Definitions
1. Confirmed Security Breach (hereinafter, "Confirmed Breach") means any confirmed

unauthorized exposure, loss of control, compromise, exfiltration, manipulation, disclosure, acquisition, or accessing of any Covered Information System or any DOJ Information accessed by, retrievable from, processed by, stored on, or transmitted within, to or from any such system.

2. Potential Security Breach (hereinafter, "Potential Breach") means any suspected, but unconfirmed, Covered Information System Security Breach.

3. Security Incident means any Confirmed or Potential Covered Information System Security Breach.

B. Confirmed Breach. Contractor shall immediately (and in no event later than within 1 hour of discovery) report any Confirmed Breach to the DOJ CO and the CO's Representative ("COR"). If the Confirmed Breach occurs outside of regular business hours and/or neither the DOJ CO nor the COR can be reached, Contractor must call DOJ-CERT at 1-866-US4-CERT (1-866-874-2378) immediately (and in no event later than within 1 hour of discovery of the Confirmed Breach), and shall notify the CO and COR as soon as practicable.

C. Potential Breach.

1. Contractor shall report any Potential Breach within 72 hours of detection to the DOJ CO and the COR, unless Contractor has

(a) completed its investigation of the Potential Breach in accordance with its own internal policies and procedures for identification, investigation and mitigation of Security Incidents and

(b) determined that there has been no Confirmed Breach.

2. If Contractor has not made a determination within 72 hours of detection of the Potential Breach whether an Confirmed Breach has occurred, Contractor shall report the Potential Breach to the DOJ CO and COR within one-hour (i.e., 73 hours from detection of the Potential Breach). If the time by which to report the Potential Breach occurs outside of regular business hours and/or neither the DOJ CO nor the COR can be reached, Contractor must call the DOJ Computer Emergency Readiness Team (DOJ-CERT) at

1-866-US4-CERT (1-866-874-2378) within one-hour (i.e., 73 hours from detection of the Potential Breach) and contact the DOJ CO and COR as soon as practicable.

D. Any report submitted in accordance with paragraphs (B) and (C), above, shall identify (1) both the Information Systems and DOJ Information involved or at risk, including the type, amount, and level of sensitivity of the DOJ Information and, if the DOJ Information contains PII, the estimated number of unique instances of PII, (2) all steps and processes being undertaken by Contractor to minimize, remedy, and/or investigate the Security Incident, (3) any and all other information as required by the US-CERT Federal Incident Notification Guidelines, including the functional impact, information impact, impact to recoverability, threat vector, mitigation details, and all available incident details; and (4) any other information specifically requested by the DOJ. Contractor shall continue to provide written updates to the DOJ CO regarding the status of the Security Incident at least every three (3) calendar days until informed otherwise by the DOJ CO.

E. All determinations regarding whether and when to notify individuals and/or federal agencies potentially affected by a Security Incident will be made by DOJ senior officials or the DOJ Core Management Team at DOJ's discretion.

F. Upon notification of a Security Incident in accordance with this section, Contractor must provide to DOJ full access to any affected or potentially affected facility and/or Information System, including access by the DOJ OIG and Federal law enforcement organizations, and undertake any and all response actions DOJ determines are required to ensure the protection of DOJ Information, including providing all requested images, log files, and event information to facilitate rapid resolution of any Security Incident.

G. DOJ, at its sole discretion, may obtain, and Contractor will permit, the assistance of other federal agencies and/or third party contractors or firms to aid in response activities related to any Security Incident. Additionally, DOJ, at its sole discretion, may require Contractor to retain, at Contractor's expense, a Third Party Assessing Organization (3PAO), acceptable to DOJ, with expertise in incident response, compromise assessment, and federal security control requirements, to conduct a thorough vulnerability and security assessment of all affected Information Systems.

H. Response activities related to any Security Incident undertaken by DOJ, including activities undertaken by Contractor, other federal agencies, and any third-party contractors or firms at the request or direction of DOJ, may include inspections, investigations, forensic reviews, data analyses and processing, and final determinations of responsibility for the Security Incident and/or liability for any additional response activities. Contractor shall be responsible for all costs and related resource allocations required for all such response activities related to

any Security Incident, including the cost of any penetration testing.

VII. Personally Identifiable Information Notification Requirement

Contractor certifies that it has a security policy in place that contains procedures to promptly notify any individual whose Personally Identifiable Information ("PII") was, or is reasonably determined by DOJ to have been, compromised. Any notification shall be co-ordinated with the DOJ CO and shall not proceed until the DOJ has made a determination that notification would not impede a law enforcement investigation or jeopardize national security. The method and content of any notification by Contractor shall be coordinated with, and subject to the approval of, DOJ.

Contractor shall be responsible for taking corrective action consistent with DOJ Data Breach Notification Procedures and as directed by the DOJ CO, including all costs and expenses associated with such corrective action, which may include providing credit monitoring to any individuals whose PII was actually or potentially compromised.

VIII. Pass-through of Security Requirements to Subcontractors and CSPs

The requirements set forth in the preceding paragraphs of this clause apply to all subcontractors and CSPs who perform work in connection with this Contract, including any CSP providing services for any other CSP under this Contract, and Contractor shall flow down this clause to all subcontractors and CSPs performing under this contract. Any breach by any subcontractor or CSP of any of the provisions set forth in this clause will be attributed to Contractor.

(End of Clause)

Addendum ATF-49 ATF-49 Security Of Information And Information Systems, Including Personally identifiable Data (PII) (Revised April 8, 2016)

I. Axon will not delete Agency Content for 90-days following termination. There will be no functionality of Axon Cloud Services during these 90-days other than the ability to retrieve Agency Content. Agency will not incur additional fees if Agency downloads Agency Content from Axon Cloud Services during this time. Axon has no obligation to maintain or provide Agency Content after these 90-days and will thereafter, unless legally prohibited, delete all Agency Content. Upon request, Axon will provide written proof that Axon successfully deleted and fully removed all Agency Content from Axon Cloud Services.

Section H Special Contract Requirements (ATF & DOJ Clauses)

52.204-24 REPRESENTATION REGARDING CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT (DEC 2019)

The Offeror shall not complete the representation in this provision if the Offeror has represented that it "does not provide covered telecommunications equipment or services as a part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument" in the provision at 52.204-26, Covered Telecommunications Equipment or Services--Representation, or in paragraph (v) of the provision at 52.212-3, Offeror Representations and Certifications--Commercial Items.

(a) *Definitions.* As used in this provision--

"Covered telecommunications equipment or services", "critical technology", and "substantial or essential component" have the meanings provided in clause 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

(b) *Prohibition.* Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. Contractors are not prohibited from providing--

(1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(c) *Procedures.* The Offeror shall review the list of excluded parties in the System for Award Management (SAM) (<https://www.sam.gov>) for entities excluded from receiving federal awards for "covered telecommunications equipment or services".

(d) *Representation.* The Offeror represents that it will, will not provide covered telecommunications equipment or services to the Government in the performance of any contract, subcontract or other contractual instrument resulting from this solicitation.

(e) *Disclosures.* If the Offeror has represented in paragraph (d) of this provision that it "will" provide covered telecommunications equipment or services", the Offeror shall provide the following information as part of the offer--

(1) A description of all covered telecommunications equipment and services offered (include brand; model number, such as original equipment manufacturer (OEM) number, manufacturer part number, or wholesaler number; and item description, as applicable);

(2) Explanation of the proposed use of covered telecommunications equipment and services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b) of this provision;

(3) For services, the entity providing the covered telecommunications services (include entity name, unique entity identifier, and Commercial and Government Entity (CAGE) code, if known); and

(4) For equipment, the entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the OEM or a distributor, if known).

(End of provision)

52.204-26 COVERED TELECOMMUNICATIONS EQUIPMENT OR SERVICES- REPRESENTATION (OCT 2020)

(a) *Definitions.* As used in this provision, "covered telecommunications equipment or services" and "reasonable inquiry" have the meaning provided in the clause 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

(b) *Procedures.* The Offeror shall review the list of excluded parties in the System for Award Management (SAM) (<https://www.sam.gov>) for entities excluded from receiving federal awards for "covered telecommunications equipment or services".

(c) *Representations.*

(1) The Offeror represents that it does, does not provide covered telecommunications equipment or services as a part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument.

(2) After conducting a reasonable inquiry for purposes of this representation, the offeror represents that it does, does not use covered telecommunications equipment or services, or any equipment, system, or service that uses covered telecommunications equipment or services.

(End of provision)

52.209-11 REPRESENTATION BY CORPORATIONS REGARDING DELINQUENT TAX LIABILITY OR A FELONY

(a) As required by sections 744 and 745 of Division E of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235), and similar provisions, if contained in subsequent appropriations acts, the Government will not enter into a contract with any corporation that--

(1) Has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability, where the awarding agency is aware of the unpaid tax liability, unless an agency has considered suspension or debarment of the corporation and made a determination that suspension or debarment is not necessary to protect the interests of the Government; or

(2) Was convicted of a felony criminal violation under any Federal law within the preceding 24 months, where the awarding agency is aware of the conviction, unless an agency has considered suspension or debarment of the corporation and made a determination that this action is not necessary to protect the interests of the Government.

(b) The Offeror represents that--

(1) It is is not a corporation that has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability; and

(2) It is is not a corporation that was convicted of a felony criminal violation under a Federal law within the preceding 24 months.

(End of provision)

52.209-11 REPRESENTATION BY CORPORATIONS REGARDING DELINQUENT TAX LIABILITY OR A FELONY CONVICTION UNDER ANY FEDERAL LAW (FEB 2016)

52.203-3 Gratuities (Apr 1984)

(a) The right of the Contractor to proceed may be terminated by written notice if, after notice and hearing, the agency head or a designee determines that the Contractor, its agent, or another representative--

(1) Offered or gave a gratuity (*e.g.*, an entertainment or gift) to an officer, official, or employee of the Government; and

(2) Intended, by the gratuity, to obtain a contract or favorable treatment under a contract.

(b) The facts supporting this determination may be reviewed by any court having lawful jurisdiction.

(c) If this contract is terminated under paragraph (a) of this clause, the Government is entitled--

(1) To pursue the same remedies as in a breach of the contract; and

(2) In addition to any other damages provided by law, to exemplary damages of not less than 3 nor more than 10 times the cost incurred by the Contractor in giving gratuities to the person concerned, as determined by the agency head or a designee. (This paragraph (c)(2) is applicable only if this contract uses money appropriated to the Department of Defense.)

(d) The rights and remedies of the Government provided in this clause shall not be exclusive and are in addition to any other rights and remedies provided by law or under this contract.

(End of clause)

52.203-5 Covenant Against Contingent Fees (May 2014)

(a) The Contractor warrants that no person or agency has been employed or retained to solicit or obtain this contract upon an agreement or understanding for a contingent fee, except a bona fide employee or agency. For breach or violation of this warranty, the Government shall have the right to annul this contract without liability or, to deduct from the contract price or consideration, or otherwise recover, the full amount of the contingent fee.

(b) "Bona fide agency," as used in this clause, means an established commercial or selling agency, maintained by a contractor for the purpose of securing business, that neither exerts nor proposes to exert improper influence to solicit or obtain Government contracts nor holds itself out as being able to obtain any Government contract or contracts through improper influence.

"Bona fide employee," as used in this clause, means a person, employed by a contractor and subject to the contractor's supervision and control as to time, place, and manner of performance, who neither exerts nor proposes to exert improper influence to solicit or obtain Government contracts nor holds out as being able to obtain any Government contract or contracts through improper influence.

"Contingent fee," as used in this clause, means any commission, percentage, brokerage, or other fee that is contingent upon the success that a person or concern has in securing a Government contract.

"Improper influence," as used in this clause, means any influence that induces or tends to induce a Government employee or officer to give consideration or to act regarding a Government contract on any basis other than the merits of the matter.

(End of clause)

52.203-7 Anti-Kickback Procedures (May 2014)

(a) *Definitions.*

"Kickback," as used in this clause, means any money, fee, commission, credit, gift, gratuity, thing of value, or compensation of any kind which is provided to any prime Contractor, prime Contractor employee, subcontractor, or subcontractor employee for the purpose of improperly obtaining or rewarding favorable treatment in connection with a prime contract or in connection with a subcontract relating to a prime contract.

"Person," as used in this clause, means a corporation, partnership, business association of any kind, trust, joint-stock company, or individual.

"Prime contract," as used in this clause, means a contract or contractual action entered into by the United States for the purpose of obtaining supplies, materials, equipment, or services of any kind.

"Prime Contractor" as used in this clause, means a person who has entered into a prime contract with the United States.

"Prime Contractor employee," as used in this clause, means any officer, partner, employee, or agent of a prime Contractor.

"Subcontract," as used in this clause, means a contract or contractual action entered into by a prime Contractor or subcontractor for the purpose of obtaining supplies, materials, equipment, or services of any kind under a prime contract.

"Subcontractor," as used in this clause, (1) means any person, other than the prime Contractor, who offers to furnish or furnishes any supplies, materials, equipment, or services of any kind under a prime contract or a subcontract entered into in connection with such prime contract, and (2) includes any person who offers to furnish or furnishes general supplies to the prime Contractor or a higher tier subcontractor.

"Subcontractor employee," as used in this clause, means any officer, partner, employee, or agent of a subcontractor.

(b) 41 U.S.C. chapter 87, Kickbacks, prohibits any person from--

(1) Providing or attempting to provide or offering to provide any kickback;

(2) Soliciting, accepting, or attempting to accept any kickback; or

(3) Including, directly or indirectly, the amount of any kickback in the contract price charged by a prime Contractor to the United States or in the contract price charged by a subcontractor to a prime Contractor or higher tier subcontractor.

(c) (1) The Contractor shall have in place and follow reasonable procedures designed to prevent and detect possible violations described in paragraph (b) of this clause in its own operations and direct business relationships.

(2) When the Contractor has reasonable grounds to believe that a violation described in paragraph (b) of this clause may have occurred, the Contractor shall promptly report in writing the possible violation. Such reports shall be made to the inspector general of the contracting agency, the head of the contracting agency if the agency does not have an inspector general, or the Attorney General.

(3) The Contractor shall cooperate fully with any Federal agency investigating a possible violation described in paragraph (b) of this clause.

(4) The Contracting Officer may (i) offset the amount of the kickback against any monies owed by the United States under the prime contract and/or (ii) direct that the Prime Contractor withhold from sums owed a subcontractor under the prime contract the amount of the kickback. The Contracting Officer may order that monies withheld under subdivision (c)(4)(ii) of this clause be paid over to the Government unless the Government has already offset those monies under subdivision (c)(4)(i) of this clause. In either case, the Prime Contractor shall notify the Contracting Officer when the monies are withheld.

(5) The Contractor agrees to incorporate the substance of this clause, including paragraph (c)(5) but excepting paragraph (c)(1), in all subcontracts under this contract which exceed \$150,000.

(End of clause)

52.203-12 Limitation On Payments To Influence Certain Federal Transactions (Oct 2010)

(a) *Definitions.* As used in this clause--

"Agency" means "executive agency" as defined in Federal Acquisition Regulation (FAR) 2.101.

"Covered Federal action" means any of the following actions:

(1) Awarding any Federal contract.

(2) Making any Federal grant.

(3) Making any Federal loan.

(4) Entering into any cooperative agreement.

(5) Extending, continuing, renewing, amending, or modifying any Federal contract, grant, loan, or cooperative agreement.

"Indian tribe" and "tribal organization" have the meaning provided in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 450b) and include Alaskan Natives.

"Influencing or attempting to influence" means making, with the intent to influence, any communication to or appearance before an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with any covered Federal action.

"Local government" means a unit of government in a State and, if chartered, established, or otherwise recognized by a State for the performance of a governmental duty, including a local public authority, a special district, an intrastate district, a council of governments, a sponsor group representative organization, and any other instrumentality of a local government.

"Officer or employee of an agency" includes the following individuals who are employed by an agency:

(1) An individual who is appointed to a position in the Government under Title 5, United States Code, including a position under a temporary appointment.

(2) A member of the uniformed services, as defined in subsection 101(3), Title 37, United States Code.

(3) A special Government employee, as defined in section 202, Title 18, United States Code.

(4) An individual who is a member of a Federal advisory committee, as defined by the Federal Advisory Committee Act, Title 5, United States Code, appendix 2.

"Person" means an individual, corporation, company, association, authority, firm, partnership, society, State, and local government, regardless of whether such entity is operated for profit, or not for profit. This term excludes an Indian tribe, tribal organization, or any other Indian organization eligible to receive Federal contracts, grants, cooperative agreements, or loans from an agency, but only with respect to expenditures by such tribe or organization that are made for purposes specified in paragraph (b) of this clause and are permitted by other Federal law.

"Reasonable compensation" means, with respect to a regularly employed officer or employee of any person, compensation that is consistent with the normal compensation for such officer or employee for work that is not furnished to, not funded by, or not furnished in cooperation with the Federal Government.

"Reasonable payment" means, with respect to professional and other technical services, a payment in an amount that is consistent with the amount normally paid for such services in the private sector.

"Recipient" includes the Contractor and all subcontractors. This term excludes an Indian tribe, tribal organization, or any other Indian organization eligible to receive Federal contracts, grants, cooperative agreements, or loans from an agency, but only with respect to expenditures by such tribe or organization that are made for purposes specified in paragraph (b) of this clause and are permitted by other Federal law.

"Regularly employed" means, with respect to an officer or employee of a person requesting or receiving a Federal contract, an officer or employee who is employed by such person for at least 130 working days within 1 year immediately preceding the date of the submission that initiates agency consideration of such person for receipt of such contract. An officer or employee who is employed by such person for less than 130 working days within 1 year immediately preceding the date of the submission that initiates agency consideration of such person shall be considered to be regularly employed as soon as he or she is employed by such person for 130 working days.

"State" means a State of the United States, the District of Columbia, or an outlying area of the United States, an agency or instrumentality of a State, and multi-State, regional, or interstate entity having governmental duties and powers.

(b) *Prohibition.* 31 U.S.C. 1352 prohibits a recipient of a Federal contract, grant, loan, or cooperative agreement from using appropriated funds to pay any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with any covered Federal

actions. In accordance with 31 U.S.C. 1352 the Contractor shall not use appropriated funds to pay any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the award of this contract the extension, continuation, renewal, amendment, or modification of this contract.

(1) The term appropriated funds does not include profit or fee from a covered Federal action.

(2) To the extent the Contractor can demonstrate that the Contractor has sufficient monies, other than Federal appropriated funds, the Government will assume that these other monies were spent for any influencing activities that would be unallowable if paid for with Federal appropriated funds.

(c) *Exceptions.* The prohibition in paragraph (b) of this clause does not apply under the following conditions:

(1) Agency and legislative liaison by Contractor employees. (i) Payment of reasonable compensation made to an officer or employee of the Contractor if the payment is for agency and legislative liaison activities not directly related to this contract. For purposes of this paragraph, providing any information specifically requested by an agency or Congress is permitted at any time.

(ii) Participating with an agency in discussions that are not related to a specific solicitation for any covered Federal action, but that concern--

(A) The qualities and characteristics (including individual demonstrations) of the person's products or services, conditions or terms of sale, and service capabilities; or

(B) The application or adaptation of the person's products or services for an agency's use.

(iii) Providing prior to formal solicitation of any covered Federal action any information not specifically requested but necessary for an agency to make an informed decision about initiation of a covered Federal action;

(iv) Participating in technical discussions regarding the preparation of an unsolicited proposal prior to its official submission; and

(v) Making capability presentations prior to formal solicitation of any covered Federal action by persons seeking awards from an agency pursuant to the provisions of the Small Business Act, as amended by Pub. L. 95-507, and subsequent amendments.

(2) Professional and technical services. (i) A payment of reasonable compensation made to an officer or employee of a person requesting or receiving a covered Federal action or an extension, continuation, renewal, amendment, or modification of a covered Federal action, if payment is for professional or technical services rendered directly in the preparation, submission, or negotiation of any bid, proposal, or application for that Federal action or for meeting requirements imposed by or pursuant to law as a condition for receiving that Federal action.

(ii) Any reasonable payment to a person, other than an officer or employee of a person requesting or receiving a covered Federal action or an extension, continuation, renewal, amendment, or modification of a covered Federal action if the payment is for professional or technical services rendered directly in the preparation, submission, or negotiation of any bid, proposal, or application for that Federal action or for meeting requirements imposed by or pursuant to law as a condition for receiving that Federal action. Persons other than officers or employees of a person requesting or receiving a covered Federal action include consultants and trade associations.

(iii) As used in paragraph (c)(2) of this clause, "professional and technical services" are limited to advice and analysis directly applying any professional or technical discipline (for examples, see FAR 3.803(a)(2)(iii)).

(iv) Requirements imposed by or pursuant to law as a condition for receiving a covered Federal award include those required by law or regulation and any other requirements in the actual award documents.

(3) Only those communications and services expressly authorized by paragraphs (c)(1) and (2) of this clause are permitted.

(d) *Disclosure.* (1) If the Contractor did not submit OMB Standard Form LLL, Disclosure of Lobbying Activities, with its offer, but registrants under the Lobbying Disclosure Act of 1995 have subsequently made a lobbying contact on behalf of the Contractor with respect to this contract, the Contractor shall complete and submit OMB Standard Form LLL to provide the name of the lobbying registrants, including the individuals performing the services.

(2) If the Contractor did submit OMB Standard Form LLL disclosure pursuant to paragraph (d) of the provision at FAR 52.203-11, Certification and Disclosure Regarding Payments to Influence Certain Federal Transactions, and a change occurs that affects Block 10 of the OMB Standard Form LLL (name and address of lobbying registrant or individuals performing services), the Contractor shall, at the end of the calendar quarter in which the change occurs, submit to the Contracting Officer within 30 days an updated disclosure using OMB Standard Form LLL.

(e) *Penalties.* (1) Any person who makes an expenditure prohibited under paragraph (b) of this clause or who fails to file or amend the disclosure to be filed or amended by paragraph (d) of this clause shall be subject to civil penalties as provided for by 31 U.S.C. 1352. An imposition of a civil penalty does not prevent the Government from seeking any other remedy that may be applicable.

(2) Contractors may rely without liability on the representation made by their subcontractors in the certification and disclosure form.

(f) *Cost allowability.* Nothing in this clause makes allowable or reasonable any costs which would otherwise be unallowable or unreasonable. Conversely, costs made specifically unallowable by the requirements in this clause will not be made allowable under any other provision.

(g) *Subcontracts.* (1) The Contractor shall obtain a declaration, including the certification and disclosure in paragraphs (c) and (d) of the provision at FAR 52.203-11, Certification and Disclosure Regarding Payments to Influence Certain Federal Transactions, from each person requesting or receiving a subcontract exceeding \$150,000 under this contract. The Contractor or subcontractor that awards the subcontract shall retain the declaration.

(2) A copy of each subcontractor disclosure form (but not certifications) shall be forwarded from tier to tier until received by the prime Contractor. The prime Contractor shall, at the end of the calendar quarter in which the disclosure form is submitted by the subcontractor, submit to the Contracting Officer within 30 days a copy of all disclosures. Each subcontractor certification shall be retained in the subcontract file of the awarding Contractor.

(3) The Contractor shall include the substance of this clause, including this paragraph (g), in any subcontract exceeding \$150,000.

(End of clause)

52.203-17 Contractor Employee Whistleblower Rights and Requirement To Inform Employees of Whistleblower Rights (Apr 2014)

(a) This contract and employees working on this contract will be subject to the whistleblower rights and remedies in the pilot program on Contractor employee whistleblower protections established at 41 U.S.C. 4712 by section 828 of the National Defense Authorization Act for Fiscal Year 2013 (Pub. L. 112-239) and FAR 3.908.

(b) The Contractor shall inform its employees in writing, in the predominant language of the workforce, of employee whistleblower rights and protections under 41 U.S.C. 4712, as described in section 3.908 of the Federal Acquisition Regulation.

(c) The Contractor shall insert the substance of this clause, including this paragraph (c), in all subcontracts over the simplified acquisition threshold.

(End of clause)

52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (Aug 2019)

(a) *Definitions.* As used in this clause--

"Covered foreign country" means The People's Republic of China.

"Covered telecommunications equipment or services" means--

(1) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);

(2) For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);

(3) Telecommunications or video surveillance services provided by such entities or using such equipment; or

(4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

"Critical technology" means--

(1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;

(2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled--

(i) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or

(ii) For reasons relating to regional stability or surreptitious listening;

(3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);

(4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);

(5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or

(6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817).

"Substantial or essential component" means any component necessary for the proper function or performance of a piece of equipment, system, or service.

(b) *Prohibition.* Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The Contractor is prohibited from providing to the Government any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in Federal Acquisition Regulation 4.2104.

(c) *Exceptions.* This clause does not prohibit contractors from providing--

(1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(d) *Reporting requirement.*

(1) In the event the Contractor identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report the information in paragraph (d)(2) of this clause to the Contracting Officer, unless elsewhere in this contract are established procedures for reporting the information; in the case of the Department of Defense, the Contractor shall report to the website at <https://dibnet.dod.mil>. For indefinite delivery contracts, the Contractor shall report to the Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) for any affected

order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at <https://dibnet.dod.mil>.

(2) The Contractor shall report the following information pursuant to paragraph (d)(1) of this clause

(i) Within one business day from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; supplier unique entity identifier (if known); supplier Commercial and Government Entity (CAGE) code (if known); brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the information in paragraph (d)(2)(i) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of covered telecommunications equipment or services, and any additional efforts that will be incorporated to prevent future use or submission of covered telecommunications equipment or services.

(e) *Subcontracts*. The Contractor shall insert the substance of this clause, including this paragraph (e), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

(End of clause)

52.215-19 Notification of Ownership Changes (Oct 1997)

(a) The Contractor shall make the following notifications in writing:

(1) When the Contractor becomes aware that a change in its ownership has occurred, or is certain to occur, that could result in changes in the valuation of its capitalized assets in the accounting records, the Contractor shall notify the Administrative Contracting Officer (ACO) within 30 days.

(2) The Contractor shall also notify the ACO within 30 days whenever changes to asset valuations or any other cost changes have occurred or are certain to occur as a result of a change in ownership.

(b) The Contractor shall--

(1) Maintain current, accurate, and complete inventory records of assets and their costs;

(2) Provide the ACO or designated representative ready access to the records upon request;

(3) Ensure that all individual and grouped assets, their capitalized values, accumulated depreciation or amortization, and remaining useful lives are identified accurately before and after each of the Contractor's ownership changes; and

(4) Retain and continue to maintain depreciation and amortization schedules based on the asset records maintained before each Contractor ownership change.

(c) The Contractor shall include the substance of this clause in all subcontracts under this contract that meet the applicability requirement of FAR 15.408(k).

(End of clause)

52.217-8 Option to Extend Services (Nov 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within _____ [insert the period of time within which the Contracting Officer may exercise the option].

(End of clause)

52.227-1 Authorization and Consent (Dec 2007)

(a) The Government authorizes and consents to all use and manufacture, in performing this contract or any subcontract at any tier, of any invention described in and covered by a United States patent--

(1) Embodied in the structure or composition of any article the delivery of which is accepted by the Government under this contract; or

(2) Used in machinery, tools, or methods whose use necessarily results from compliance by the Contractor or a subcontractor with (i) specifications or written provisions forming a part of this contract or (ii) specific written instructions given by the Contracting Officer directing the manner of performance. the entire liability to the Government for infringement of a United States patent shall be determined solely by the provisions of the indemnity clause, if any, included in this contract or any subcontract hereunder (including any lower-tier subcontract), and the Government assumes liability for all other infringement to the extent of the authorization and consent hereinabove granted.

(b) The Contractor shall include the substance of this clause, including this paragraph (b), in all subcontracts that are expected to exceed the simplified acquisition threshold. However, omission of this clause from any subcontract, including those at or below the simplified acquisition threshold, does not affect this authorization and consent.

(End of clause)

52.227-2 Notice and Assistance Regarding Patent and Copyright Infringement (Dec 2007)

(a) The Contractor shall report to the Contracting Officer, promptly and in reasonable written detail, each notice or claim of patent or copyright infringement based on the performance of this contract of which the Contractor has knowledge.

(b) In the event of any claim or suit against the Government on account of any alleged patent or copyright infringement arising out of the performance of this contract or out of the use of any supplies furnished or work or services performed under this contract, the Contractor shall furnish to the Government, when requested by the Contracting Officer, all evidence and information in the Contractor's possession pertaining to such claim or suit. Such evidence and information shall be furnished at the expense of the Government except where the Contractor has agreed to indemnify the Government.

(c) The Contractor shall include the substance of this clause, including this paragraph (c), in all subcontracts that are expected to exceed the simplified acquisition threshold.

(End of clause)

52.227-14 Rights in Data-General (May 2014)

(a) *Definitions.* As used in this clause--

"Computer database" or "database means" a collection of recorded information in a form capable of, and for the purpose of, being stored in, processed, and operated on by a computer. The term does not include computer software.

"Computer software"--

(1) *Means*

(i) Computer programs that comprise a series of instructions, rules, routines, or statements, regardless of the media in which recorded, that allow or cause a computer to perform a specific operation or series of operations; and

(ii) Recorded information comprising source code listings, design details, algorithms, processes, flow charts, formulas, and related material that would enable the computer program to be produced, created, or compiled.

(2) Does not include computer databases or computer software documentation.

"Computer software documentation" means owner's manuals, user's manuals, installation instructions, operating instructions, and other similar items, regardless of storage medium, that explain the capabilities of the computer software or provide instructions for using the software.

"Data" means recorded information, regardless of form or the media on which it may be recorded. The term includes technical data and computer software. The term does not include information incidental to contract administration, such as financial, administrative, cost or pricing, or management information.

"Form, fit, and function data" means data relating to items, components, or processes that are sufficient to enable physical and functional interchangeability, and data identifying source, size, configuration, mating and attachment characteristics, functional characteristics, and performance requirements. For computer software it means data identifying source, functional characteristics, and performance requirements but specifically excludes the source code, algorithms, processes, formulas, and flow charts of the software.

"Limited rights" means the rights of the Government in limited rights data as set forth in the Limited Rights Notice of paragraph (g)(3) if included in this clause.

"Limited rights data" means data, other than computer software, that embody trade secrets or are commercial or financial and confidential or privileged, to the extent that such data pertain to items, components, or processes developed at private expense, including minor modifications.

"Restricted computer software" means computer software developed at private expense and that is a trade secret, is commercial or financial and confidential or privileged, or is copyrighted computer software, including minor modifications of the computer software.

"Restricted rights," as used in this clause, means the rights of the Government in restricted computer software, as set forth in a Restricted Rights Notice of paragraph (g) if included in this clause, or as otherwise may be provided in a collateral agreement incorporated in and made part of this contract, including minor modifications of such computer software.

"Technical data" means recorded information (regardless of the form or method of the recording) of a scientific or technical nature (including computer databases and computer software documentation). This term does not include computer software or financial, administrative, cost or pricing, or management data or other information incidental to contract administration. The term includes recorded information of a scientific or technical nature that is included in computer databases. (See 41 U.S.C. 116).

"Unlimited rights" means the rights of the Government to use, disclose, reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, in any manner and for any purpose, and to have or permit others to do so.

(b) Allocation of rights.

(1) Except as provided in paragraph (c) of this clause, the Government shall have unlimited rights in--

(i) Data first produced in the performance of this contract;

(ii) Form, fit, and function data delivered under this contract;

(iii) Data delivered under this contract (except for restricted computer software) that constitute manuals or instructional and training material for installation, operation, or routine maintenance and repair of items, components, or processes delivered or furnished for use under this contract; and

(iv) All other data delivered under this contract unless provided otherwise for limited rights data or restricted computer software in accordance with paragraph (g) of this clause.

(2) The Contractor shall have the right to--

(i) Assert copyright in data first produced in the performance of this contract to the extent provided in paragraph (c)(1) of this clause;

(ii) Use, release to others, reproduce, distribute, or publish any data first produced or specifically used by the Contractor in the performance of this contract, unless provided otherwise in paragraph (d) of this clause;

(iii) Substantiate the use of, add, or correct limited rights, restricted rights, or copyright notices and to take other appropriate action, in accordance with paragraphs (e) and (f) of this clause; and

(iv) Protect from unauthorized disclosure and use those data that are limited rights data or restricted computer software to the extent provided in paragraph (g) of this clause.

(c) *Copyright--*

(1) *Data first produced in the performance of this contract.*

(i) Unless provided otherwise in paragraph (d) of this clause, the Contractor may, without prior approval of the Contracting Officer, assert copyright in scientific and technical articles based on or containing data first produced in the performance of this contract and published in academic, technical or professional journals, symposia proceedings, or similar works. The prior, express written permission of the Contracting Officer is required to assert copyright in all other data first produced in the performance of this contract.

(ii) When authorized to assert copyright to the data, the Contractor shall affix the applicable copyright notices of 17 U.S.C. 401 or 402, and an acknowledgment of Government sponsorship (including contract number).

(iii) For data other than computer software, the Contractor grants to the Government, and others acting on its behalf, a paid-up, nonexclusive, irrevocable, worldwide license in such copyrighted data to reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly by or on behalf of the Government. For computer software, the Contractor grants to the Government, and others acting on its behalf, a paid-up, nonexclusive, irrevocable, worldwide license in such copyrighted computer software to reproduce, prepare derivative works, and perform publicly and display publicly (but not to distribute copies to the public) by or on behalf of the Government.

(2) *Data not first produced in the performance of this contract.* The Contractor shall not, without the prior written permission of the Contracting Officer, incorporate in data delivered under this contract any data not first produced in the performance of this contract unless the Contractor--

(i) Identifies the data; and

(ii) Grants to the Government, or acquires on its behalf, a license of the same scope as set forth in paragraph (c)(1) of this clause or, if such data are restricted computer software, the Government shall acquire a copyright license as set forth in paragraph (g)(4) of this clause (if included in this contract) or as otherwise provided in a collateral agreement incorporated in or made part of this contract.

(3) *Removal of copyright notices.* The Government will not remove any authorized copyright notices placed on data pursuant to this paragraph (c), and will include such notices on all reproductions of the data.

(d) *Release, publication, and use of data.* The Contractor shall have the right to use, release to others, reproduce, distribute, or publish any data first produced or specifically used by the Contractor in the performance of this contract, except--

(1) As prohibited by Federal law or regulation (e.g., export control or national security laws or regulations);

(2) As expressly set forth in this contract; or

(3) If the Contractor receives or is given access to data necessary for the performance of this contract that contain restrictive markings, the Contractor shall treat the data in accordance with such markings unless specifically authorized otherwise in writing by the Contracting Officer.

(e) *Unauthorized marking of data.*

(1) Notwithstanding any other provisions of this contract concerning inspection or acceptance, if any data delivered under this contract are marked with the notices specified in paragraph (g)(3) or (g)(4) if included in this clause, and use of the notices is not authorized by this clause, or if the data bears any other restrictive or limiting markings not authorized by this contract, the Contracting Officer may at any time either return the data to the Contractor, or cancel or ignore the markings. However, pursuant to 41 U.S.C. 4703, the following procedures shall apply prior to canceling or ignoring the markings.

(i) The Contracting Officer will make written inquiry to the Contractor affording the Contractor 60 days from receipt of the inquiry to provide written justification to substantiate the propriety of the markings;

(ii) If the Contractor fails to respond or fails to provide written justification to substantiate the propriety of the markings within the 60-day period (or a longer time approved in writing by the Contracting Officer for good cause shown), the Government shall have

the right to cancel or ignore the markings at any time after said period and the data will no longer be made subject to any disclosure prohibitions.

(iii) If the Contractor provides written justification to substantiate the propriety of the markings within the period set in paragraph (e)(1)(i) of this clause, the Contracting Officer will consider such written justification and determine whether or not the markings are to be cancelled or ignored. If the Contracting Officer determines that the markings are authorized, the Contractor will be so notified in writing. If the Contracting Officer determines, with concurrence of the head of the contracting activity, that the markings are not authorized, the Contracting Officer will furnish the Contractor a written determination, which determination will become the final agency decision regarding the appropriateness of the markings unless the Contractor files suit in a court of competent jurisdiction within 90 days of receipt of the Contracting Officer's decision. The Government will continue to abide by the markings under this paragraph (e)(1)(iii) until final resolution of the matter either by the Contracting Officer's determination becoming final (in which instance the Government will thereafter have the right to cancel or ignore the markings at any time and the data will no longer be made subject to any disclosure prohibitions), or by final disposition of the matter by court decision if suit is filed.

(2) The time limits in the procedures set forth in paragraph (e)(1) of this clause may be modified in accordance with agency regulations implementing the Freedom of Information Act (5 U.S.C. 552) if necessary to respond to a request thereunder.

(3) Except to the extent the Government's action occurs as the result of final disposition of the matter by a court of competent jurisdiction, the Contractor is not precluded by paragraph (e) of the clause from bringing a claim, in accordance with the Disputes clause of this contract, that may arise as the result of the Government removing or ignoring authorized markings on data delivered under this contract.

(f) Omitted or incorrect markings.

(1) Data delivered to the Government without any restrictive markings shall be deemed to have been furnished with unlimited rights. The Government is not liable for the disclosure, use, or reproduction of such data.

(2) If the unmarked data has not been disclosed without restriction outside the Government, the Contractor may request, within 6 months (or a longer time approved by the Contracting Officer in writing for good cause shown) after delivery of the data, permission to have authorized notices placed on the data at the Contractor's expense. The Contracting Officer may agree to do so if the Contractor--

(i) Identifies the data to which the omitted notice is to be applied;

(ii) Demonstrates that the omission of the notice was inadvertent;

(iii) Establishes that the proposed notice is authorized; and

(iv) Acknowledges that the Government has no liability for the disclosure, use, or reproduction of any data made prior to the addition of the notice or resulting from the omission of the notice.

(3) If data has been marked with an incorrect notice, the Contracting Officer may--

(i) Permit correction of the notice at the Contractor's expense if the Contractor identifies the data and demonstrates that the correct notice is authorized; or

(ii) Correct any incorrect notices.

(g) Protection of limited rights data and restricted computer software. (1) The Contractor may withhold from delivery qualifying limited rights data or restricted computer software that are not data identified in paragraphs (b)(1)(i), (ii), and (iii) of this clause. As a condition to this withholding, the Contractor shall--

(i) Identify the data being withheld; and

(ii) Furnish form, fit, and function data instead.

(2) Limited rights data that are formatted as a computer database for delivery to the Government shall be treated as limited rights data and not restricted computer software.

(3) [Reserved]

(h) *Subcontracting*. The Contractor shall obtain from its subcontractors all data and rights therein necessary to fulfill the Contractor's obligations to the Government under this contract. If a subcontractor refuses to accept terms affording the Government those rights, the Contractor shall promptly notify the Contracting Officer of the refusal and shall not proceed with the subcontract award without authorization in writing from the Contracting Officer.

(i) *Relationship to patents or other rights*. Nothing contained in this clause shall imply a license to the Government under any patent or be construed as affecting the scope of any license or other right otherwise granted to the Government.

(End of clause)

52.229-4 Federal, State and Local Taxes (State and Local Adjustments) (Feb 2013)

(a) As used in this clause-

"After-imposed tax" means any new or increased Federal, State, or local tax or duty, or tax that was excluded on the contract date but whose exclusion was later revoked or amount of exemption reduced during the contract period, other than an excepted tax, on the transactions or property covered by this contract that the Contractor is required to pay or bear as the result of legislative, judicial, or administrative action taking effect after the contract date.

"After-relieved tax" means any amount of Federal, State, or local tax or duty, other than an excepted tax, that would otherwise have been payable on the transactions or property covered by this contract, but which the Contractor is not required to pay or bear, or for which the Contractor obtains a refund or drawback, as the result of legislative, judicial, or administrative action taking effect after the contract date.

"All applicable Federal, State, and local taxes and duties" means all taxes and duties, in effect on the contract date, that the taxing authority is imposing and collecting on the transactions or property covered by this contract.

"Contract date" means the effective date of this contract and, for any modification to this contract, the effective date of the modification.

"Excepted tax" means social security or other employment taxes, net income and franchise taxes, excess profits taxes, capital stock taxes, transportation taxes, unemployment compensation taxes, and property taxes. "Excepted tax" does not include gross income taxes levied on or measured by sales or receipts from sales, property taxes assessed on completed supplies covered by this contract, or any tax assessed on the Contractor's possession of, interest in, or use of property, title to which is in the Government.

"Local taxes" includes taxes imposed by a possession or territory of the United States, Puerto Rico, or the Northern Mariana Islands, if the contract is performed wholly or partly in any of those areas.

(b)(1) Unless otherwise provided in this contract, the contract price includes all applicable Federal, State, and local taxes and duties, except as provided in subparagraph (b)(2)(i) of this clause.

(2) Taxes imposed under 26 U.S.C. 5000C may not be --

(i) Included in the contract price; nor

(ii) Reimbursed.

(c) The contract price shall be increased by the amount of any after-imposed tax, or of any tax or duty specifically excluded from the contract price by a term or condition of this contract that the Contractor is required to pay or bear, including any interest or penalty, if the Contractor states in writing that the contract price does not include any contingency for such tax and if liability for such tax, interest, or penalty was not incurred through the Contractor's fault, negligence, or failure to follow instructions of the Contracting Officer.

(d) The contract price shall be decreased by the amount of any after-relieved tax. The Government shall be entitled to interest received by the Contractor incident to a refund of taxes to the extent that such interest was earned after the Contractor was paid by the Government for such taxes. The Government shall be entitled to repayment of any penalty refunded to the Contractor to the extent that the penalty was paid by the Government.

(e) The contract price shall be decreased by the amount of any Federal, State, or local tax, other than an excepted tax, that was included in the contract price and that the Contractor is required to pay or bear, or does not obtain a refund of, through the Contractor's fault, negligence, or failure to follow instructions of the Contracting Officer.

(f) No adjustment shall be made in the contract price under this clause unless the amount of the adjustment exceeds \$250.

(g) The Contractor shall promptly notify the Contracting Officer of all matters relating to Federal, State, and local taxes and duties that reasonably may be expected to result in either an increase or decrease in the contract price and shall take appropriate action as the Contracting Officer directs. The contract price shall be equitably adjusted to cover the costs of action taken by the Contractor at the direction of the Contracting Officer, including any interest, penalty, and reasonable attorneys' fees.

(h) The Government shall furnish evidence appropriate to establish exemption from any Federal, State, or local tax when-

(1) The Contractor requests such exemption and states in writing that it applies to a tax excluded from the contract price; and

(2) A reasonable basis exists to sustain the exemption.

(End of clause)

52.232-1 Payments (Apr 1984)

The Government shall pay the Contractor, upon the submission of proper invoices or vouchers, the prices stipulated in this contract for supplies delivered and accepted or services rendered and accepted, less any deductions provided in this contract. Unless otherwise specified in this contract, payment shall be made on partial deliveries accepted by the Government if--

(a) The amount due on the deliveries warrants it; or

(b) The Contractor requests it and the amount due on the deliveries is at least \$1,000 or 50 percent of the total contract price.

(End of clause)

52.232-39 Unenforceability of Unauthorized Obligations (Jun 2013)

(a) Except as stated in paragraph (b) of this clause, when any supply or service acquired under this contract is subject to any End User License Agreement (EULA), Terms of Service (TOS), or similar legal instrument or agreement, that includes any clause requiring the Government to indemnify the Contractor or any person or entity for damages, costs, fees, or any other loss or liability that would create an Anti-Deficiency Act violation (31 U.S.C. 1341), the following shall govern:

(1) Any such clause is unenforceable against the Government.

(2) Neither the Government nor any Government authorized end user shall be deemed to have agreed to such clause by virtue of it appearing in the EULA, TOS, or similar legal instrument or agreement. If the EULA, TOS, or similar legal instrument or agreement is invoked through an "I agree" click box or other comparable mechanism (e.g., "click-wrap" or "browse-wrap" agreements), execution does not bind the Government or any Government authorized end user to such clause.

(3) Any such clause is deemed to be stricken from the EULA, TOS, or similar legal instrument or agreement.

(b) Paragraph (a) of this clause does not apply to indemnification by the Government that is expressly authorized by statute and specifically authorized under applicable agency regulations and procedures.

(End of clause)

52.233-3 Protest after Award (Aug 1996)

(a) Upon receipt of a notice of protest (as defined in FAR 33.101) or a determination that a protest is likely (see FAR 33.102(d)), the Contracting Officer may, by written order to the Contractor, direct the Contractor to stop performance of the work called for by this contract. The order shall be specifically identified as a stop-work order issued under this clause. Upon receipt of the order, the Contractor shall immediately comply with its terms and take all reasonable steps to minimize the incurrence of costs allocable to

the work covered by the order during the period of work stop-page. Upon receipt of the final decision in the protest, the Contracting Officer shall either--

(1) Cancel the stop-work order; or

(2) Terminate the work covered by the order as provided in the Default, or the Termination for Convenience of the Government, clause of this contract.

(b) If a stop-work order issued under this clause is canceled either before or after a final decision in the protest, the Contractor shall resume work. The Contracting Officer shall make an equitable adjustment in the delivery schedule or contract price, or both, and the contract shall be modified, in writing, accordingly, if--

(1) The stop-work order results in an increase in the time required for, or in the Contractor's cost properly allocable to, the performance of any part of this contract; and

(2) The Contractor asserts its right to an adjustment within 30 days after the end of the period of work stoppage; *provided*, that if the Contracting Officer decides the facts justify the action, the Contracting Officer may receive and act upon a proposal at any time before final payment under this contract.

(c) If a stop-work order is not canceled and the work covered by the order is terminated for the convenience of the Government, the Contracting Officer shall allow reasonable costs resulting from the stop-work order in arriving at the termination settlement.

(d) If a stop-work order is not canceled and the work covered by the order is terminated for default, the Contracting Officer shall allow, by equitable adjustment or otherwise, reasonable costs resulting from the stop-work order.

(e) The Government's rights to terminate this contract at any time are not affected by action taken under this clause.

(f) If, as the result of the Contractor's intentional or negligent misstatement, misrepresentation, or miscertification, a protest related to this contract is sustained, and the Government pays costs, as provided in FAR 33.102(b)(2) or 33.104(h)(1), the Government may require the Contractor to reimburse the Government the amount of such costs. In addition to any other remedy available, and pursuant to the requirements of subpart 32.6, the Government may collect this debt by offsetting the amount against any payment due the Contractor under any contract between the Contractor and the Government.

(End of clause)

52.233-3 Alt I Protest after Award (Aug 1996) - Alternate I (Jun 1985)

(a) Upon receipt of a notice of protest (as defined in FAR 33.101) or a determination that a protest is likely (see FAR 33.102(d)), the Contracting Officer may, by written order to the Contractor, direct the Contractor to stop performance of the work called for by this contract. The order shall be specifically identified as a stop-work order issued under this clause. Upon receipt of the order, the Contractor shall immediately comply with its terms and take all reasonable steps to minimize the incurrence of costs allocable to the work covered by the order during the period of work stop-page. Upon receipt of the final decision in the protest, the Contracting Officer shall either--

(1) Cancel the stop-work order; or

(2) Terminate the work covered by the order as *provided* in the Termination clause of this contract.

(b) If a stop-work order issued under this clause is canceled either before or after a final decision in the protest, the Contractor shall resume work. The Contracting Officer shall make an equitable adjustment in the delivery schedule, the estimated cost, the fee, or a combination thereof, and in any other terms of the contract that may be affected, and the contract shall be modified, in writing, accordingly, if--

(1) The stop-work order results in an increase in the time required for, or in the Contractor's cost properly allocable to, the performance of any part of this contract; and

(2) The Contractor asserts its right to an adjustment within 30 days after the end of the period of work stoppage; *provided*, that if the Contracting Officer decides the facts justify the action, the Contracting Officer may receive and act upon a proposal at any time before final payment under this contract.

(c) If a stop-work order is not canceled and the work covered by the order is terminated for the convenience of the Government, the Contracting Officer shall allow reasonable costs resulting from the stop-work order in arriving at the termination settlement.

(d) If a stop-work order is not canceled and the work covered by the order is terminated for default, the Contracting Officer shall allow, by equitable adjustment or otherwise, reasonable costs resulting from the stop-work order.

(e) The Government's rights to terminate this contract at any time are not affected by action taken under this clause.

(f) If, as the result of the Contractor's intentional or negligent misstatement, misrepresentation, or miscertification, a protest related to this contract is sustained, and the Government pays costs, as provided in FAR 33.102(b)(2) or 33.104(h)(1), the Government may require the Contractor to reimburse the Government the amount of such costs. In addition to any other remedy available, and pursuant to the requirements of subpart 32.6, the Government may collect this debt by offsetting the amount against any payment due the Contractor under any contract between the Contractor and the Government.

(End of clause)

52.242-1 Notice of Intent to Disallow Costs (Apr 1984)

(a) Notwithstanding any other clause of this contract--

(1) The Contracting Officer may at any time issue to the Contractor a written notice of intent to disallow specified costs incurred or planned for incurrence under this contract that have been determined not to be allowable under the contract terms; and

(2) The Contractor may, after receiving a notice under paragraph (a)(1) of this clause, submit a written response to the Contracting Officer, with justification for allowance of the costs. If the Contractor does respond within 60 days, the Contracting Officer shall, within 60 days of receiving the response, either make a written withdrawal of the notice or issue a written decision.

(b) Failure to issue a notice under this Notice of Intent to Disallow Costs clause shall not affect the Government's rights to take exception to incurred costs.

(End of clause)

52.243-1 Changes-Fixed-Price (Aug 1987)

(a) The Contracting Officer may at any time, by written order, and without notice to the sureties, if any, make changes within the general scope of this contract in any one or more of the following:

(1) Drawings, designs, or specifications when the supplies to be furnished are to be specially manufactured for the Government in accordance with the drawings, designs, or specifications.

(2) Method of shipment or packing.

(3) Place of delivery.

(b) If any such change causes an increase or decrease in the cost of, or the time required for, performance of any part of the work under this contract, whether or not changed by the order, the Contracting Officer shall make an equitable adjustment in the contract price, the delivery schedule, or both, and shall modify the contract.

(c) The Contractor must assert its right to an adjustment under this clause within 30 days from the date of receipt of the written order. However, if the Contracting Officer decides that the facts justify it, the Contracting Officer may receive and act upon a proposal submitted before final payment of the contract.

(d) If the Contractor's proposal includes the cost of property made obsolete or excess by the change, the Contracting Officer shall have the right to prescribe the manner of the disposition of the property.

(e) Failure to agree to any adjustment shall be a dispute under the Disputes clause. However, nothing in this clause shall excuse the Contractor from proceeding with the contract as changed.

(End of clause)

52.243-1 Alt II Changes-Fixed-Price (Aug 1987) - Alternate II (Apr 1984)

(a) The Contracting Officer may at any time, by written order, and without notice to the sureties, if any, make changes within the general scope of this contract in any one or more of the following:

(1) Description of services to be performed.

(2) Time of performance (*i.e.*, hours of the day, days of the week, etc.).

(3) Place of performance of the services.

(4) Drawings, designs, or specifications when the supplies to be furnished are to be specially manufactured for the Government, in accordance with the drawings, designs, or specifications.

(5) Method of shipment or packing of supplies.

(6) Place of delivery

(b) If any such change causes an increase or decrease in the cost of, or the time required for, performance of any part of the work under this contract, whether or not changed by the order, the Contracting Officer shall make an equitable adjustment in the contract price, the delivery schedule, or both, and shall modify the contract.

(c) The Contractor must assert its right to an adjustment under this clause within 30 days from the date of receipt of the written order. However, if the Contracting Officer decides that the facts justify it, the Contracting Officer may receive and act upon a proposal submitted before final payment of the contract.

(d) If the Contractor's proposal includes the cost of property made obsolete or excess by the change, the Contracting Officer shall have the right to prescribe the manner of the disposition of the property.

(e) Failure to agree to any adjustment shall be a dispute under the Disputes clause. However, nothing in this clause shall excuse the Contractor from proceeding with the contract as changed.

(End of clause)

52.246-24 Limitation of Liability-High-Value Items (Feb 1997)

(a) Except as provided in paragraphs (b) through (e) of this clause, and notwithstanding any other provision of this contract, the Contractor shall not be liable for loss of or damage to property of the Government (including the supplies delivered under this contract) that-

(1) Occurs after Government acceptance of the supplies delivered under this contract; and

(2) Results from any defects or deficiencies in the supplies.

(b) The limitation of liability under paragraph (a) of this clause shall not apply when a defect or deficiency in, or the Government's acceptance of, the supplies results from willful misconduct or lack of good faith on the part of any of the Contractor's managerial personnel. The term "Contractor's managerial personnel," as used in this clause, means the Contractor's directors, officers, and any of the Contractor's managers, superintendents, or equivalent representatives who have supervision or direction of-

(1) All or substantially all of the Contractor's business;

(2) All or substantially all of the Contractor's operations at any one plant, laboratory, or separate location at which the contract is being performed; or

(3) A separate and complete major industrial operation connected with the performance of this contract.

(c) If the Contractor carries insurance, or has established a reserve for self-insurance, covering liability for loss or damage suffered by the Government through purchase or use of the supplies required to be delivered under this contract, the Contractor shall be liable to the Government, to the extent of such insurance or reserve, for loss of or damage to property of the Government occurring after Government acceptance of, and resulting from any defects or deficiencies in, the supplies delivered under this contract.

(d)(1) This clause does not diminish the Contractor's obligations, to the extent that they arise otherwise under this contract, relating to correction, repair, replacement, or other relief for any defect or deficiency in supplies delivered under this contract.

(2) Unless this is a cost-reimbursement contract, if loss or damage occurs and correction, repair, or replacement is not feasible or desired by the Government, the Contractor shall, as determined by the Contracting Officer-

(i) Pay the Government the amount it would have cost the Contractor to make correction, repair, or replacement before the loss or damage occurred;

(ii) Provide other equitable relief.

(e) This clause shall not limit or otherwise affect the Government's rights under clauses, if included in this contract, that cover-

(1) Warranty of technical data;

(2) Ground and flight risks or aircraft flight risks; or

(3) Government property.

(End of clause)

52.249-2 Termination for Convenience of the Government (Fixed-Price) (Apr 2012)

(a) The Government may terminate performance of work under this contract in whole or, from time to time, in part if the Contracting Officer determines that a termination is in the Government's interest. The Contracting Officer shall terminate by delivering to the Contractor a Notice of Termination specifying the extent of termination and the effective date.

(b) After receipt of a Notice of Termination, and except as directed by the Contracting Officer, the Contractor shall immediately proceed with the following obligations, regardless of any delay in determining or adjusting any amounts due under this clause:

(1) Stop work as specified in the notice.

(2) Place no further subcontracts or orders (referred to as subcontracts in this clause) for materials, services, or facilities, except as necessary to complete the continued portion of the contract.

(3) Terminate all subcontracts to the extent they relate to the work terminated.

(4) Assign to the Government, as directed by the Contracting Officer, all right, title, and interest of the Contractor under the subcontracts terminated, in which case the Government shall have the right to settle or to pay any termination settlement proposal arising out of those terminations.

(5) With approval or ratification to the extent required by the Contracting Officer, settle all outstanding liabilities and termination settlement proposals arising from the termination of subcontracts; the approval or ratification will be final for purposes of this clause.

(6) As directed by the Contracting Officer, transfer title and deliver to the Government--

(i) The fabricated or unfabricated parts, work in process, completed work, supplies, and other material produced or acquired for the work terminated; and

(ii) The completed or partially completed plans, drawings, information, and other property that, if the contract had been completed, would be required to be furnished to the Government.

(7) Complete performance of the work not terminated.

(8) Take any action that may be necessary, or that the Contracting Officer may direct, for the protection and preservation of the property related to this contract that is in the possession of the Contractor and in which the Government has or may acquire an interest.

(9) Use its best efforts to sell, as directed or authorized by the Contracting Officer, any property of the types referred to in paragraph (b)(6) of this clause; *provided*, however, that the Contractor (i) is not required to extend credit to any purchaser and (ii) may acquire the property under the conditions prescribed by, and at prices approved by, the Contracting Officer. The proceeds of any transfer or disposition will be applied to reduce any payments to be made by the Government under this contract, credited to the price or cost of the work, or paid in any other manner directed by the Contracting Officer.

(c) The Contractor shall submit complete termination inventory schedules no later than 120 days from the effective date of termination, unless extended in writing by the Contracting Officer upon written request of the Contractor within this 120-day period.

(d) After expiration of the plant clearance period as defined in Subpart 49.001 of the Federal Acquisition Regulation, the Contractor may submit to the Contracting Officer a list, certified as to quantity and quality, of termination inventory not previously disposed of, excluding items authorized for disposition by the Contracting Officer. The Contractor may request the Government to remove those items or enter into an agreement for their storage. Within 15 days, the Government will accept title to those items and remove them or enter into a storage agreement. The Contracting Officer may verify the list upon removal of the items, or if stored, within 45 days from submission of the list, and shall correct the list, as necessary, before final settlement.

(e) After termination, the Contractor shall submit a final termination settlement proposal to the Contracting Officer in the form and with the certification prescribed by the Contracting Officer. The Contractor shall submit the proposal promptly, but no later than 1 year from the effective date of termination, unless extended in writing by the Contracting Officer upon written request of the Contractor within this 1-year period. However, if the Contracting Officer determines that the facts justify it, a termination settlement proposal may be received and acted on after 1 year or any extension. If the Contractor fails to submit the proposal within the time allowed, the Contracting Officer may determine, on the basis of information available, the amount, if any, due the Contractor because of the termination and shall pay the amount determined.

(f) Subject to paragraph (e) of this clause, the Contractor and the Contracting Officer may agree upon the whole or any part of the amount to be paid or remaining to be paid because of the termination. The amount may include a reasonable allowance for profit on work done. However, the agreed amount, whether under this paragraph (f) or paragraph (g) of this clause, exclusive of costs shown in paragraph (g)(3) of this clause, may not exceed the total contract price as reduced by (1) the amount of payments previously made and (2) the contract price of work not terminated. The contract shall be modified, and the Contractor paid the agreed amount. Paragraph (g) of this clause shall not limit, restrict, or affect the amount that may be agreed upon to be paid under this paragraph.

(g) If the Contractor and the Contracting Officer fail to agree on the whole amount to be paid because of the termination of work, the Contracting Officer shall pay the Contractor the amounts determined by the Contracting Officer as follows, but without duplication of any amounts agreed on under paragraph (f) of this clause:

(1) The contract price for completed supplies or services accepted by the Government (or sold or acquired under paragraph (b)(9) of this clause) not previously paid for, adjusted for any saving of freight and other charges.

(2) The total of--

(i) The costs incurred in the performance of the work terminated, including initial costs and preparatory expense allocable thereto, but excluding any costs attributable to supplies or services paid or to be paid under paragraph (g)(1) of this clause;

(ii) The cost of settling and paying termination settlement proposals under terminated subcontracts that are properly chargeable to the terminated portion of the contract if not included in subdivision (g)(2)(i) of this clause; and

(iii) A sum, as profit on subdivision (g)(2)(i) of this clause, determined by the Contracting Officer under 49.202 of the Federal Acquisition Regulation, in effect on the date of this contract, to be fair and reasonable; however, if it appears that the Contractor would have sustained a loss on the entire contract had it been completed, the Contracting Officer shall allow no profit under this subdivision (g)(2)(iii) and shall reduce the settlement to reflect the indicated rate of loss.

(3) The reasonable costs of settlement of the work terminated, including--

(i) Accounting, legal, clerical, and other expenses reasonably necessary for the preparation of termination settlement proposals and supporting data;

(ii) The termination and settlement of subcontracts (excluding the amounts of such settlements); and

(iii) Storage, transportation, and other costs incurred, reasonably necessary for the preservation, protection, or disposition of the termination inventory.

(h) Except for normal spoilage, and except to the extent that the Government expressly assumed the risk of loss, the Contracting Officer shall exclude from the amounts payable to the Contractor under paragraph (g) of this clause, the fair value as determined by the Contracting Officer, for the loss of the Government property.

(i) The cost principles and procedures of part 31 of the Federal Acquisition Regulation, in effect on the date of this contract, shall govern all costs claimed, agreed to, or determined under this clause.

(j) The Contractor shall have the right of appeal, under the Disputes clause, from any determination made by the Contracting Officer under paragraph (e), (g), or (l) of this clause, except that if the Contractor failed to submit the termination settlement proposal or request for equitable adjustment within the time provided in paragraph (e) or (l), respectively, and failed to request a time extension, there is no right of appeal.

(k) In arriving at the amount due the Contractor under this clause, there shall be deducted--

(1) All unliquidated advance or other payments to the Contractor under the terminated portion of this contract;

(2) Any claim which the Government has against the Contractor under this contract; and

(3) The agreed price for, or the proceeds of sale of, materials, supplies, or other things acquired by the Contractor or sold under the provisions of this clause and not recovered by or credited to the Government.

(l) If the termination is partial, the Contractor may file a proposal with the Contracting Officer for an equitable adjustment of the price(s) of the continued portion of the contract. The Contracting Officer shall make any equitable adjustment agreed upon. Any proposal by the Contractor for an equitable adjustment under this clause shall be requested within 90 days from the effective date of termination unless extended in writing by the Contracting Officer.

(m) (1) The Government may, under the terms and conditions it prescribes, make partial payments and payments against costs incurred by the Contractor for the terminated portion of the contract, if the Contracting Officer believes the total of these payments will not exceed the amount to which the Contractor will be entitled.

(2) If the total payments exceed the amount finally determined to be due, the Contractor shall repay the excess to the Government upon demand, together with interest computed at the rate established by the Secretary of the Treasury under 50 U.S.C. App. 1215(b) (2). Interest shall be computed for the period from the date the excess payment is received by the Contractor to the date the excess is repaid. Interest shall not be charged on any excess payment due to a reduction in the Contractor's termination settlement proposal because of retention or other disposition of termination inventory until 10 days after the date of the retention or disposition, or a later date determined by the Contracting Officer because of the circumstances.

(n) Unless otherwise provided in this contract or by statute, the Contractor shall maintain all records and documents relating to the terminated portion of this contract for 3 years after final settlement. This includes all books and other evidence bearing on the Contractor's costs and expenses under this contract. The Contractor shall make these records and documents available to the Government, at the Contractor's office, at all reasonable times, without any direct charge. If approved by the Contracting Officer, photographs, microphotographs, or other authentic reproductions may be maintained instead of original records and documents.

(End of clause)

52.249-8 Default (Fixed-Price Supply and Service) (Apr 1984)

(a)(1) The Government may, subject to paragraphs (c) and (d) of this clause, by written notice of default to the Contractor, terminate this contract in whole or in part if the Contractor fails to--

(i) Deliver the supplies or to perform the services within the time specified in this contract or any extension;

(ii) Make progress, so as to endanger performance of this contract (but see paragraph (a)(2) of this clause); or

(iii) Perform any of the other provisions of this contract (but see paragraph (a)(2) of this clause).

(2) The Government's right to terminate this contract under subdivisions (a)(1)(ii) and (1)(iii) of this clause, may be exercised if the Contractor does not cure such failure within 10 days (or more if authorized in writing by the Contracting Officer) after receipt of the notice from the Contracting Officer specifying the failure.

(b) If the Government terminates this contract in whole or in part, it may acquire, under the terms and in the manner the Contracting Officer considers appropriate, supplies or services similar to those terminated, and the Contractor will be liable to the Government for any excess costs for those supplies or services. However, the Contractor shall continue the work not terminated.

(c) Except for defaults of subcontractors at any tier, the Contractor shall not be liable for any excess costs if the failure to perform the contract arises from causes beyond the control and without the fault or negligence of the Contractor. Examples of such causes include (1) acts of God or of the public enemy, (2) acts of the Government in either its sovereign or contractual capacity, (3) fires, (4) floods, (5) epidemics, (6) quarantine restrictions, (7) strikes, (8) freight embargoes, and (9) unusually severe weather. In each instance the failure to perform must be beyond the control and without the fault or negligence of the Contractor.

(d) If the failure to perform is caused by the default of a subcontractor at any tier, and if the cause of the default is beyond the control of both the Contractor and subcontractor, and without the fault or negligence of either, the Contractor shall not be liable for any excess costs for failure to perform, unless the subcontracted supplies or services were obtainable from other sources in sufficient time for the Contractor to meet the required delivery schedule.

(e) If this contract is terminated for default, the Government may require the Contractor to transfer title and deliver to the Government, as directed by the Contracting Officer, any (1) completed supplies, and (2) partially completed supplies and materials, parts, tools, dies, jigs, fixtures, plans, drawings, information, and contract rights (collectively referred to as "manufacturing materials" in this clause) that the Contractor has specifically produced or acquired for the terminated portion of this contract. Upon direction of the Contracting Officer, the Contractor shall also protect and preserve property in its possession in which the Government has an interest.

(f) The Government shall pay contract price for completed supplies delivered and accepted. The Contractor and Contracting Officer shall agree on the amount of payment for manufacturing materials delivered and accepted and for the protection and preservation of the property. Failure to agree will be a dispute under the Disputes clause. The Government may withhold from these amounts any sum the Contracting Officer determines to be necessary to protect the Government against loss because of outstanding liens or claims of former lien holders.

(g) If, after termination, it is determined that the Contractor was not in default, or that the default was excusable, the rights and obligations of the parties shall be the same as if the termination had been issued for the convenience of the Government.

(h) The rights and remedies of the Government in this clause are in addition to any other rights and remedies provided by law or under this contract.

(End of clause)

52.249-8 Alt I Default (Fixed-Price Supply and Service) (Apr 1984) - Alternate I (Apr 1984)

(a) (1) The Government may, subject to paragraphs (c) and (d) of this clause, by written notice of default to the Contractor, terminate this contract in whole or in part if the Contractor fails to--

(i) Pick up the commodities or to perform the services, including delivery services, within the time specified in this contract or any extension;

(ii) Make progress, so as to endanger performance of this contract (but see paragraph (a)(2) of this clause); or

(iii) Perform any of the other provisions of this contract (but see paragraph (a)(2) of this clause).

(2) The Government's right to terminate this contract under subdivisions (a)(1)(ii) and (iii) of this clause, may be exercised if the Contractor does not cure such failure within 10 days (or more if authorized in writing by the Contracting Officer) after receipt of the notice from the Contracting Officer specifying the failure.

(b) If the Government terminates this contract in whole or in part, it may acquire, under the terms and in the manner the Contracting Officer considers appropriate, supplies or services similar to those terminated, and the Contractor will be liable to the Government for any excess costs for those supplies or services. However, the Contractor shall continue the work not terminated.

(c) Except for defaults of subcontractors at any tier, the Contractor shall not be liable for any excess costs if the failure to perform the contract arises from causes beyond the control and without the fault or negligence of the Contractor. Examples of such causes include (1) acts of God or of the public enemy, (2) acts of the Government in either its sovereign or contractual capacity, (3) fires, (4) floods, (5) epidemics, (6) quarantine restrictions, (7) strikes, (8) freight embargoes, and (9) unusually severe weather. In each instance the failure to perform must be beyond the control and without the fault or negligence of the Contractor.

(d) If the failure to perform is caused by the default of a subcontractor at any tier, and if the cause of the default is beyond the control of both the Contractor and subcontractor, and without the fault or negligence of either, the Contractor shall not be liable for any excess costs for failure to perform, unless the subcontracted supplies or services were obtainable from other sources in sufficient time for the Contractor to meet the required delivery schedule.

(e) If this contract is terminated while the Contractor has possession of Government goods, the Contractor shall, upon direction of the Contracting Officer, protect and preserve the goods until surrendered to the Government or its agent. The Contractor and Contracting Officer shall agree on payment for the preservation and protection of goods. Failure to agree on an amount will be a dispute under the Disputes clause.

(f) If, after termination, it is determined that the Contractor was not in default, or that the default was excusable, the rights and obligations of the parties shall be the same as if the termination had been issued for the convenience of the Government.

(g) The rights and remedies of the Government in this clause are in addition to any other rights and remedies provided by law or under this contract.

(End of clause)

[END OF ADDENDUM TO FAR 52.212-4]

52.212-5 Contract Terms and Conditions Required to Implement Statutes or Executive Orders--
Commercial Items (Oct 2019)

(a) The Contractor shall comply with the following Federal Acquisition Regulation (FAR) clauses, which are incorporated in this contract by reference, to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

(1) 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).

(2) 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Jul 2018) (Section 1634 of Pub. L. 115-91).

(3) 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (Aug 2019) (Section 889(a)(1)(A) of Pub. L. 115-232).

(4) 52.209-10, Prohibition on Contracting with Inverted Domestic Corporations (Nov 2015).

(5) 52.233-3, Protest After Award (Aug 1996) (31 U.S.C. 3553).

(6) 52.233-4, Applicable Law for Breach of Contract Claim (Oct 2004)(Public Laws 108-77 and 108-78 (19 U.S.C. 3805 note)).

(b) The Contractor shall comply with the FAR clauses in this paragraph (b) that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

[Contracting Officer check as appropriate.]

__ (1) 52.203-6, Restrictions on Subcontractor Sales to the Government (Sept 2006), with Alternate I (Oct 1995) (41 U.S.C. 4704 and 10 U.S.C. 2402).

__ (2) 52.203-13, Contractor Code of Business Ethics and Conduct (Oct 2015) (41 U.S.C. 3509)).

- ___ (3) 52.203-15, Whistleblower Protections under the American Recovery and Reinvestment Act of 2009 (June 2010) (Section 1553 of Pub. L. 111-5). (Applies to contracts funded by the American Recovery and Reinvestment Act of 2009.)
- ___ (4) 52.204-10, Reporting Executive Compensation and First-Tier Subcontract Awards (Oct 2018) (Pub. L. 109-282) (31 U.S.C. 6101 note).
- ___ (5) [Reserved].
- ___ (6) 52.204-14, Service Contract Reporting Requirements (Oct 2016) (Pub. L. 111-117, section 743 of Div. C).
- ___ (7) 52.204-15, Service Contract Reporting Requirements for Indefinite-Delivery Contracts (Oct 2016) (Pub. L. 111-117, section 743 of Div. C).
- ___ (8) 52.209-6, Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment. (Oct 2015) (31 U.S.C. 6101 note).
- ___ (9) 52.209-9, Updates of Publicly Available Information Regarding Responsibility Matters (Oct 2018) (41 U.S.C. 2313).
- ___ (10) [Reserved].
- ___ (11)(i) 52.219-3, Notice of HUBZone Set-Aside or Sole-Source Award (Nov 2011) (15 U.S.C. 657a).
- ___ (ii) Alternate I (Nov 2011) of 52.219-3.
- ___ (12)(i) 52.219-4, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (Oct 2014) (if the offeror elects to waive the preference, it shall so indicate in its offer) (15 U.S.C. 657a).
- ___ (ii) Alternate I (Jan 2011) of 52.219-4.
- ___ (13) [Reserved]
- ___ (14)(i) 52.219-6, Notice of Total Small Business Set-Aside (Nov 2011) (15 U.S.C. 644).
- ___ (ii) Alternate I (Nov 2011).
- ___ (iii) Alternate II (Nov 2011).
- ___ (15)(i) 52.219-7, Notice of Partial Small Business Set-Aside (June 2003) (15 U.S.C. 644).
- ___ (ii) Alternate I (Oct 1995) of 52.219-7.
- ___ (iii) Alternate II (Mar 2004) of 52.219-7.
- ___ (16) 52.219-8, Utilization of Small Business Concerns (Oct 2018) (15 U.S.C. 637(d)(2) and (3)).
- ___ (17)(i) 52.219-9, Small Business Subcontracting Plan (Aug 2018) (15 U.S.C. 637(d)(4)).
- ___ (ii) Alternate I (Nov 2016) of 52.219-9.
- ___ (iii) Alternate II (Nov 2016) of 52.219-9.
- ___ (iv) Alternate III (Nov 2016) of 52.219-9.
- ___ (v) Alternate IV (Aug 2018) of 52.219-9.
- ___ (18) 52.219-13, Notice of Set-Aside of Orders (Nov 2011) (15 U.S.C. 644(r)).
- ___ (19) 52.219-14, Limitations on Subcontracting (Jan 2017) (15 U.S.C. 637(a)(14)).

- ☐ (20) 52.219-16, Liquidated Damages--Subcon-tracting Plan (Jan 1999) (15 U.S.C. 637(d)(4)(F)(i)).
- ☐ (21) 52.219-27, Notice of Service-Disabled Veteran-Owned Small Business Set-Aside (Oct 2019) (15 U.S.C. 657f).
- ☐ (22) 52.219-28, Post Award Small Business Program Rerepresentation (Jul 2013) (15 U.S.C. 632(a)(2)).
- ☐ (23) 52.219-29, Notice of Set-Aside for, or Sole Source Award to, Economically Disadvantaged Women-Owned Small Business Concerns (Dec 2015) (15 U.S.C. 637(m)).
- ☐ (24) 52.219-30, Notice of Set-Aside for, or Sole Source Award to, Women-Owned Small Business Concerns Eligible Under the Women-Owned Small Business Program (Dec 2015) (15 U.S.C. 637(m)).
- ☒ (25) 52.222-3, Convict Labor (June 2003) (E.O. 11755).
- ☒ (26) 52.222-19, Child Labor--Cooperation with Authorities and Remedies (Oct 2019) (E.O. 13126).
- ☒ (27) 52.222-21, Prohibition of Segregated Facilities (Apr 2015).
- ☒ (28)(i) 52.222-26, Equal Opportunity (Sept 2016) (E.O. 11246).
- ☐ (ii) Alternate I (Feb 1999) of 52.222-26.
- ☒ (29)(i) 52.222-35, Equal Opportunity for Veterans (Oct 2015)(38 U.S.C. 4212).
- ☐ (ii) Alternate I (July 2014) of 52.222-35.
- ☒ (30)(i) 52.222-36, Equal Opportunity for Workers with Disabilities (July 2014) (29 U.S.C. 793).
- ☐ (ii) Alternate I (July 2014) of 52.222-36.
- ☒ (31) 52.222-37, Employment Reports on Veterans (Feb 2016) (38 U.S.C. 4212).
- ☐ (32) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496).
- ☐ (33)(i) 52.222-50, Combating Trafficking in Persons (Jan 2019) (22 U.S.C. chapter 78 and E.O. 13627).
- ☐ (ii) Alternate I (Mar 2015) of 52.222-50 (22 U.S.C. chapter 78 and E.O. 13627).
- ☐ (34) 52.222-54, Employment Eligibility Verification (Oct 2015). (Executive Order 12989). (Not applicable to the acquisition of commercially available off-the-shelf items or certain other types of commercial items as prescribed in 22.1803.)
- ☐ (35)(i) 52.223-9, Estimate of Percentage of Recovered Material Content for EPA-Designated Items (May 2008) (42 U.S.C. 6962(c) (3)(A)(ii)). (Not applicable to the acquisition of commercially available off-the-shelf items.)
- ☐ (ii) Alternate I (May 2008) of 52.223-9 (42 U.S.C. 6962(i)(2)(C)). (Not applicable to the acquisition of commercially available off-the-shelf items.)
- ☐ (36) 52.223-11, Ozone-Depleting Substances and High Global Warming Potential Hydrofluorocarbons (Jun 2016) (E.O. 13693).
- ☐ (37) 52.223-12, Maintenance, Service, Repair, or Disposal of Refrigeration Equipment and Air Conditioners (Jun 2016) (E.O. 13693).
- ☐ (38)(i) 52.223-13, Acquisition of EPEAT®-Registered Imaging Equipment (Jun 2014) (E.O.s 13423 and 13514).
- ☐ (ii) Alternate I (Oct 2015) of 52.223-13.
- ☐ (39)(i) 52.223-14, Acquisition of EPEAT®-Registered Televisions (Jun 2014) (E.O.s 13423 and 13514).
- ☐ (ii) Alternate I (Jun 2014) of 52.223-14.

- ☐ (40) 52.223-15, Energy Efficiency in Energy-Consuming Products (Dec 2007) (42 U.S.C. 8259b).
- ☐ (41)(i) 52.223-16, Acquisition of EPEAT®-Registered Personal Computer Products (Oct 2015) (E.O.s 13423 and 13514).
- ☐ (ii) Alternate I (Jun 2014) of 52.223-16.
- ☒ (42) 52.223-18, Encouraging Contractor Policies to Ban Text Messaging While Driving (Aug 2011) (E.O. 13513).
- ☐ (43) 52.223-20, Aerosols (Jun 2016) (E.O. 13693).
- ☐ (44) 52.223-21, Foams (Jun 2016) (E.O. 13693).
- ☐ (45)(i) 52.224-3, Privacy Training (Jan 2017) (5 U.S.C. 552a).
- ☐ (ii) Alternate I (Jan 2017) of 52.224-3.
- ☐ (46) 52.225-1, Buy American--Supplies (May 2014) (41 U.S.C. chapter 83).
- ☐ (47)(i) 52.225-3, Buy American--Free Trade Agreements--Israeli Trade Act (May 2014) (41 U.S.C. chapter 83, 19 U.S.C. 3301 note, 19 U.S.C. 2112 note, 19 U.S.C. 3805 note, 19 U.S.C. 4001 note, Pub. L. 103-182, 108-77, 108-78, 108-286, 108-302, 109-53, 109-169, 109-283, 110-138, 112-41, 112-42, and 112-43).
- ☐ (ii) Alternate I (May 2014) of 52.225-3.
- ☐ (iii) Alternate II (May 2014) of 52.225-3.
- ☐ (iv) Alternate III (May 2014) of 52.225-3.
- ☐ (48) 52.225-5, Trade Agreements (Oct 2019) (19 U.S.C. 2501, et seq., 19 U.S.C. 3301 note).
- ☐ (49) 52.225-13, Restrictions on Certain Foreign Purchases (June 2008) (E.O.'s, proclamations, and statutes administered by the Office of Foreign Assets Control of the Department of the Treasury).
- ☐ (50) 52.225-26, Contractors Performing Private Security Functions Outside the United States (Oct 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).
- ☐ (51) 52.226-4, Notice of Disaster or Emergency Area Set-Aside (Nov 2007) (42 U.S.C. 5150).
- ☐ (52) 52.226-5, Restrictions on Subcontracting Outside Disaster or Emergency Area (Nov 2007) (42 U.S.C. 5150).
- ☐ (53) 52.232-29, Terms for Financing of Purchases of Commercial Items (Feb 2002) (41 U.S.C. 4505, 10 U.S.C. 2307(f)).
- ☐ (54) 52.232-30, Installment Payments for Commercial Items (Jan 2017) (41 U.S.C. 4505, 10 U.S.C. 2307(f)).
- ☒ (55) 52.232-33, Payment by Electronic Funds Transfer--System for Award Management (Oct 2018) (31 U.S.C. 3332).
- ☐ (56) 52.232-34, Payment by Electronic Funds Transfer--Other than System for Award Management (Jul 2013) (31 U.S.C. 3332).
- ☐ (57) 52.232-36, Payment by Third Party (May 2014) (31 U.S.C. 3332).
- ☐ (58) 52.239-1, Privacy or Security Safeguards (Aug 1996) (5 U.S.C. 552a).
- ☐ (59) 52.242-5, Payments to Small Business Subcontractors (Jan 2017)(15 U.S.C. 637(d)(13)).
- ☐ (60)(i) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx. 1241(b) and 10 U.S.C. 2631).
- ☐ (ii) Alternate I (Apr 2003) of 52.247-64.
- ☐ (iii) Alternate II (Feb 2006) of 52.247-64.

(c) The Contractor shall comply with the FAR clauses in this paragraph (c), applicable to commercial services, that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

[Contracting Officer check as appropriate.]

__ (1) 52.222-17, Nondisplacement of Qualified Workers (May 2014)(E.O. 13495).

__ (2) 52.222-41, Service Contract Labor Standards (Aug 2018) (41 U.S.C. chapter 67).

__ (3) 52.222-42, Statement of Equivalent Rates for Federal Hires (May 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

__ (4) 52.222-43, Fair Labor Standards Act and Service Contract Labor Standards-Price Adjustment (Multiple Year and Option Contracts) (Aug 2018) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

__ (5) 52.222-44, Fair Labor Standards Act and Service Contract Labor Standards--Price Adjustment (May 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

__ (6) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment--Requirements (May 2014) (41 U.S.C. chapter 67).

__ (7) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services--Requirements (May 2014) (41 U.S.C. chapter 67).

__ (8) 52.222-55, Minimum Wages Under Executive Order 13658 (Dec 2015).

__ (9) 52.222-62, Paid Sick Leave Under Executive Order 13706 (Jan 2017) (E.O. 13706).

__ (10) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations (May 2014) (42 U.S.C. 1792).

(d) *Comptroller General Examination of Record.* The Contractor shall comply with the provisions of this paragraph (d) if this contract was awarded using other than sealed bid, is in excess of the simplified acquisition threshold, and does not contain the clause at 52.215-2, Audit and Records--Negotiation.

(1) The Comptroller General of the United States, or an authorized representative of the Comptroller General, shall have access to and right to examine any of the Contractor's directly pertinent records involving transactions related to this contract.

(2) The Contractor shall make available at its offices at all reasonable times the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this contract or for any shorter period specified in FAR subpart 4.7, Contractor Records Retention, of the other clauses of this contract. If this contract is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement. Records relating to appeals under the disputes clause or to litigation or the settlement of claims arising under or relating to this contract shall be made available until such appeals, litigation, or claims are finally resolved.

(3) As used in this clause, records include books, documents, accounting procedures and practices, and other data, regardless of type and regardless of form. This does not require the Contractor to create or maintain any record that the Contractor does not maintain in the ordinary course of business or pursuant to a provision of law.

(e)(1) Notwithstanding the requirements of the clauses in paragraphs (a), (b), (c), and (d) of this clause, the Contractor is not required to flow down any FAR clause, other than those in this paragraph (e)(1) in a subcontract for commercial items. Unless otherwise indicated below, the extent of the flow down shall be as required by the clause--

(i) 52.203-13, Contractor Code of Business Ethics and Conduct (Oct 2015) (41 U.S.C. 3509).

(ii) 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).

(iii) 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Jul 2018) (Section 1634 of Pub. L. 115-91).

(iv) 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (Aug 2019) (Section 889(a)(1)(A) of Pub. L. 115-232).

(v) 52.219-8, Utilization of Small Business Concerns (Oct 2018) (15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds \$700,000 (\$1.5 million for construction of any public facility), the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.

(vi) 52.222-17, Nondisplacement of Qualified Workers (May 2014) (E.O. 13495). Flow down required in accordance with paragraph (l) of FAR clause 52.222-17.

(vii) 52.222-21, Prohibition of Segregated Facilities (Apr 2015)

(viii) 52.222-26, Equal Opportunity (Sept 2016) (E.O. 11246).

(ix) 52.222-35, Equal Opportunity for Veterans (Oct 2015) (38 U.S.C. 4212).

(x) 52.222-36, Equal Opportunity for Workers with Disabilities (Jul 2014) (29 U.S.C. 793).

(xi) 52.222-37, Employment Reports on Veterans (Feb 2016) (38 U.S.C. 4212)

(xii) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496). Flow down required in accordance with paragraph (f) of FAR clause 52.222-40.

(xiii) 52.222-41, Service Contract Labor Standards (Aug 2018) (41 U.S.C. chapter 67).

(xiv) (A) 52.222-50, Combating Trafficking in Persons (Jan 2019) (22 U.S.C. chapter 78 and E.O 13627).

(B) Alternate I (Mar 2015) of 52.222-50 (22 U.S.C. chapter 78 and E.O 13627).

(xv) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment-Requirements (May 2014) (41 U.S.C. chapter 67).

(xvi) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services-Requirements (May 2014) (41 U.S.C. chapter 67).

(xvii) 52.222-54, Employment Eligibility Verification (Oct 2015) (E.O. 12989).

(xix) 52.222-55, Minimum Wages Under Executive Order 13658 (Dec 2015).

(xviii) 52.222-62, Paid Sick Leave Under Executive Order 13706 (Jan 2017) (E.O. 13706).

(xx)(A) 52.224-3, Privacy Training (Jan 2017) (5 U.S.C. 552a).

(B) Alternate I (Jan 2017) of 52.224-3.

(xxi) 52.225-26, Contractors Performing Private Security Functions Outside the United States (Oct 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).

(xxii) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations (May 2014) (42 U.S.C. 1792). Flow down required in accordance with paragraph (e) of FAR clause 52.226-6.

(xxiii) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx. 1241(b) and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64.

(2) While not required, the Contractor may include in its subcontracts for commercial items a minimal number of additional clauses necessary to satisfy its contractual obligations.

(End of clause)

Attachment 1
Statement of Work (SOW)
Digital Evidence Management
Services

Department of Justice
Bureau of Alcohol, Tobacco, Firearms and Explosives
Special Operations Division (SOD)
Statement of Work (SOW)
November 04, 2020

1.0 BACKGROUND

The Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) is a law enforcement organization within the U.S. Department of Justice (DOJ) with unique responsibilities dedicated to reducing violent crime and protecting the public. As such, ATF enforces the federal laws and regulations relating to alcohol, tobacco, firearms, explosives, and arson by working directly and in cooperation with other federal, state, tribal and local governments, international partners, and non-governmental organizations to deter illegal firearms trafficking and violent gun crime.

Please refer to www.atf.gov for more information on ATF's mission and strategic objectives.

In the area of firearms enforcement, the ATF Strategic Plan is to reduce gun violence in the United States and fairly and effectively regulate the legitimate firearms industry. ATF's primary targets are suspects who illegally use firearms and/or supply guns to criminals and children. One tool aiding ATF in this endeavor is the Digital Evidence Management Program.

Within ATF, the Digital Evidence Management Program is located within the Special Operations Division (SOD). SOD's goal is to provide intelligence led policing and to focus ATF's limited resources with localized strategic investigative plans. Through this method, ATF will enhance its abilities to solve, reduce, and prevent firearm-related violent crime. This program uses an integrated investigative approach, which works in concert with other Federal, State, tribal and local law enforcement agencies in combating firearm-related violence through the use of technology.

The Digital Management Program also functions as a network providing the capability to share data across jurisdictional lines and discover links between crimes in different localities or different States. The use of automation in ballistic forensics is one more weapon in the arsenal of resources that ATF maintains to assist our law enforcement stakeholders.

2.0 SCOPE

The scope of this contract is to obtain a digital evidence management System/Solution/Software (DEMS) that is a one-turnkey solution with the ability functions, and features capable of supporting the ongoing operations and activities of the Digital Evidence Management Program. These Software as a Service (SaaS) licenses shall be utilized nationally by ATF personnel to support the capture, ingest, management, and secure sharing of digital evidence, to include but not limited to body-worn camera video captured from state and local partners authorized for use on federal task forces.

3.0 PERIOD OF PERFORMANCE

The period of performance of the contract shall be for one (1) 12-month base period from date of award with four (4) option years at the Government's discretion.

4.0 MANDATORY SERVICES/TASKS

4.1.Digital Evidence Management System/Software/Solution (DEMS) with Storage that:

- 4.1.1.** is a current Criminal Justice Information Services (CJIS)/FedRAMP JAB Provisional Authority to Operate (P-ATO) Authorized SaaS solution with an Authority to Operate (ATO) rated for impact level moderate certified and authorized product
- 4.1.2.** is a turnkey solution that allows for secure management, access, and sharing of digital evidence
- 4.1.3.** provides enterprise licensing permitting unlimited usage
- 4.1.4.** can accept and provide media in all forms (.jpeg, .pdf, etc.)
- 4.1.5.** provides a secure method for requesting and receiving digital content from U.S. Citizens
- 4.1.6.** has redaction capabilities powered by AI
- 4.1.7.** stores and supports various forms of third-party data ingests evidence collected from mobile phone application, Capture by Axon
- 4.1.8.** allows secure case sharing with current ATF partner agencies as well as the Executive Office of United States Attorneys (EOUSA)
- 4.1.9.** provides 2.5 petabytes of storage (10GB per 250,000)
- 4.1.10.** is a SaaS model that reduces security and administration by local IT staff: no local installation required
- 4.1.11.** has automatic, timely security upgrades and enhancements deployed to application without the need for any local IT staff involvement
- 4.1.12.** controls access to evidence based on pre-defined roles and permissions and pre-defined individuals
- 4.1.13.** has password authentication includes customizable security parameters: customizable password complexity, IP-based access restrictions, single sign-on, and multi-factor authentication support
- 4.1.14.** has automated category-based evidence retention policies assists with efficient database management in accordance with Federal Records rules of retention
- 4.1.15.** able to recover deleted evidence within seven days of deletion to ensure retention of evidence
- 4.1.16.** requires NO proprietary file formats avoiding additional cost
- 4.1.17.** able to upload files directly from the computer to Axon Evidence via an Internet browser or the Evidence Sync desktop-based application
- 4.1.18.** has data security: Robust Transport Layer Security (TLS) implementation for data in transit and 256-bit AES encryption for data in storage
- 4.1.19.** has security testing: Independent security firms perform in-depth security and penetration testing
- 4.1.20.** is reliable: Fault- and disaster-tolerant infrastructure in at least 4 redundant data centers in both the East and West regions of the United States
- 4.1.21.** has chain-of custody capabilities: Audit logs automatically track all system and user activity. These logs cannot be edited or deleted, even by account administrators and IT staff to assist in chain of custody for case prosecution
- 4.1.22.** has stability: Axon Enterprise is a publicly traded company with stable finances and funding, reducing concerns of loss of application support or commercial viability

- 4.1.23.** has a dedicated information security department that protects Axon Evidence and data with security monitoring, centralized event log analysis and correlation, advanced threat and intrusion protection, and incident response capabilities
- 4.1.24.** has evidence.com Lite for TASER Smart Weapon device management
- 4.1.25.** Storage. The Contractor shall provide 2.5 petabytes (10GB per 250,000) of storage
- 4.1.26.** License(s). The Contractor shall provide enterprise licensing capable of supporting up to 5,000 users
- 4.1.27.** Maintenance and Support. The Contractor shall provide maintenance and support in the form of case management, customer/technical support, trainings, and (on an as needed basis) associated products/services as follows:
- 4.1.28.** Case management. The Contractor shall provide program management services responsible for the scheduling and oversight of all the work performed under this contract. The program manager and a team of project managers shall be assigned to the Body Worn Camera program at the start of the contract period. The contractor's PMO shall use a project management system based on the Project Management Institute (PMI) to manage projects and activities.
- 4.1.29.** Kick-off meeting. The contractor shall schedule and coordinate a Project Kick-Off Meeting at a location and time approved by the Government. The meeting shall provide an introduction between the contractor personnel and Government personnel and provide the opportunity to discuss technical, management, transition, security issues, and reporting procedures. At a minimum, the attendees shall include key contractor personnel, the Contracting Officer and the Contracting Officer Representative (COR).
- 4.1.30.** Customer/Technical support. The contractor shall provide customer support to diagnose problems and provide solutions remotely ensuring minimal downtime that includes, but not limited to: phone-, online-, and email-based support provided during standard business hours.
- 4.1.31.** Training. The Contractor shall provide training in-person and virtually. Not to exceed \$6,000.00 per year.
- 4.1.32.** Additional Axon Products and Services. As the goals and priorities of the Digital Evidence Management Program shift and evolve, the Contractor shall provide incrementally - on an as needed basis - the additional products and services needed to support the anticipated growth of the program. Not to exceed \$250,000.00 per year.

5.0 DELIVERABLES

- 5.1** Deliverable Submissions: All electronic deliverables shall be prepared using Microsoft applications in formats selected by the contractor unless specified otherwise by the COR. All deliverables shall be delivered to the COR electronically and in hard copy. The COR will determine the method in which report deliverables are to be marked for delivery.
- 5.2** Reviews: The COR will review all draft and final deliverables within 10 business days to ensure accuracy, functionality, completeness, professional quality, and overall compliance with contract requirements. All deliverables provided by the contractor shall be accurate, current, and complete. The Government will consider errors, misleading statements, incomplete and outdated irrelevant information, excessive rhetoric, or repetition as deficiencies and the contractor shall make corrections at no additional cost.
- 5.3** Deliverables List: The list of deliverables are indicated below:

Deliverable	Format	Due Date
Kick-Off Meeting/Briefing	Contractor's standard format	Within 10 business days after contract award.
Training Schedule	To be determined (TBD) at the Kick-off Meeting/Briefing	Within 10 business days from Kick-off Meeting/Briefing.

6.0 OTHER DIRECT COSTS (ODC)

- 6.1.** ODCs may include, but are not limited to, copying, faxing, phone usage, package delivery, etc. Any single purchase, of ODCs, over \$10,000.00 is subject to FAR competition requirements. ODCs must be authorized and approved prior to any purchase by the COR.
- 6.2.** ODCs will be reimbursed for actual costs as provided in contract. To be reimbursed, invoices, including ODCs must provide a detailed breakdown of the actual expenditures invoiced, including receipts. Contractor shall maintain the original or legible copy of receipts for all ODCs invoiced. ATF reserves the right to request evidence of any ODCs requesting reimbursement. To assure timely reimbursement of ODCs, the contractor is strongly encouraged to submit charges with the monthly invoices. No profit or fee shall be applied to ODCs.

7.0 INSPECTION AND ACCEPTANCE

- 7.1.** *Inspection/Acceptance.* Supplies or services delivered under this contract shall be inspected and accepted by the COR. The Contractor shall only tender for acceptance those items that conform to the requirements of this contract. The Government reserves the right to inspect or test any supplies or services that have been tendered for acceptance in accordance with the appropriate inspection and acceptance clause.
- 7.2.** The basis for acceptance shall be compliance with the requirements/objectives/constraints set forth in the contract, and other terms and conditions of the contract. Deliverable items rejected shall be corrected in accordance with the applicable clauses.
- 7.3.** *Acceptance Criteria.* The COR will review all draft and final deliverables to ensure accuracy, functionality, completeness, professional quality, and overall compliance within the guidelines/requirements of the delivery order. The contractor shall ensure the accuracy and completeness of all deliverables. Errors, misleading or unclear statements, incomplete or irrelevant information, and or excessive rhetoric, repetition, and "padding", shall be considered deficiencies and shall be subject to correction by the contractor, at no additional cost to the Government. The contractor shall make any noted corrections/revisions, within 5 business days, after government review and comment on deliverables. If the deliverable does not meet the noted criteria, the Government will return it.
- 7.4.** *Rejection Procedures.* If the COR rejects any deliverable, that rejected document will be handled in the following manner:
- 7.5.** After notification that the deliverable did not meet the acceptance criteria, the Contractor shall resubmit an updated/corrected version within five (5) business days after receipt of Government comments.
- 7.6.** Upon re-submission by the Contractor, the Government will reapply the same acceptance criteria. If the deliverable does not meet the acceptance criteria a second time,

the Government might consider the Contractor as having deficient performance with respect to the subject task/subtask.

- 7.7. Any rework of rejected deliverables will be completed at no additional cost to the government.
- 7.8. No payments will be issued against rejected deliverables, until they are corrected and accepted by the government.

8.0 PAYMENT PROCEDURES

- 8.1. ATF requires contractors to invoice electronically on a monthly basis. Invoicing electronically saves time, money, and physical storage space for both the Government and the contractor. Each invoice must be a proper invoice in accordance with FAR 32.905(e). Electronic invoices should be submitted to the appropriate component finance office, the COR, and component POC as required. Electronic invoices will serve as the official original copy.
- 8.2. If it is determined that the amount billed is incorrect, the invoice may be revised by the Government, or the Contractor may be required to submit a revised invoice.
- 8.3. To constitute a proper invoice, each invoice must include the following information and/or documentation:
 - a) Name, address and telephone of the Contractor;
 - b) Date of invoice and invoice number;
 - c) Contract number; also modification number, if applicable; and BPA order number and its modification, if applicable;
 - d) Description of the supplies/services rendered (including hours incurred and billing rate, if applicable);
 - e) A schedule depicting the following information:
 - Amount Invoiced by Task
 - Authorized Amount by Task
 - Remaining This Period by Task
 - Cumulative Amount Invoiced by Task
 - Value of Contract Balance by Task
 - f) Name of Contracting Officer's Representative (COR);
 - g) Travel and ODCs
 - h) Signature of authorized representative of the firm with the following invoice certification:

"The undersigned hereby certifies to the best of my knowledge and belief that the sum claimed under this contract is proper and due, and all the costs of contract performance have been paid, or to the extent allowed under the applicable payment clause, **shall** be paid by the Contractor when due in the ordinary course of business; the work reflected by these costs has been performed, and amounts involved are consistent with the requirements of this contract."

BY: _____

TITLE: _____

DATE: _____

9.0 CERTIFICATION OF INVOICES

- 9.1.** The Payment Office listed on the first page of the Award Document will make payment upon receipt of an accepted and properly submitted invoice.
- 9.2.** Invoices/vouchers will be completed and submitted in accordance with the appropriate component Electronic Invoicing clause. The final invoice will be paid upon Government acceptance of the final deliverable.
- 9.3.** The COR's or component POC's certification of acceptance is an integral part of the correct invoice/voucher discussed in the "Discounts for Prompt Payment" clause, Section I (FAR Clause 52.232-8).
- 9.4.** Upon certification, the COR or component POC will forward the invoice/voucher to the Payment Office, as appropriate.
- 9.5.** The Invoice/Voucher shall include:
 - (a) Contract or other authorization number
 - (b) Product or service description.
 - (c) Quantities received, if applicable.
 - (d) Date(s) property or services accepted.
 - (e) Signature, printed name, title, phone number, and mailing address of the receiving official.
 - (f) POC to discuss invoice issues.

10.0 PAYMENT

- 10.1.** Payment for all supplies and services shall be made upon Government acceptance, in accordance with the appropriate Payments Clause, FAR 52.232-7.

11.0 INVOICE PAYMENT

- 11.1.** The address to which payment should be made is: financebranch@atf.gov.

Electronic Invoicing (June 2005)

- (a) ATF and the DOJ components strongly encourages contractors to invoice electronically. Invoicing electronically saves time, money, and physical storage space for both the Government and the contractor.
- (b) Each invoice must be a proper invoice in accordance with FAR 32.905. Contractors able to submit invoices electronically should submit each invoice to financebranch@atf.gov with a copy to the COR. Electronic invoices will serve as the official original copy. Any questions may be directed to the ATF Finance Office at (202) 648-7860. The component Finance Office's information will be documented on the component's individual BPA calls.

12.0 MANDATORY USE OF GOVERNMENT TO GOVERNMENT ELECTRONIC

MAIL. Unless exempted by the CO, in writing, communication after contract award with government agencies shall ordinarily be transmitted via electronic mail (e-mail).

- 13.0 DATA RIGHTS.** All materials, databases, software modules, source code, graphics, etc. inclusively developed and used in support of this contract shall become the property of ATF or other DOJ components.

14.0 SECTION 508 COMPLIANCE. The contractor shall deliver compliant technology solutions in accordance with Section 508 regulations and applicable accessibility standards (36 CFR Part 1194).

15.0 SYSTEM FOR AWARD MANAGEMENT (www.sam.gov).

The selected contractor must have an active registration in the SAM system prior to award in accordance with federal acquisition regulation (far) 52.204-7.

16.0 KEY PERSONNEL

16.1. The Contractor shall provide the disciplines necessary to perform the tasks listed. The Government reserves the right to reject proposed personnel if they do not meet the qualifications defined in the methodology for the positions requested. The Government will identify the key personnel positions under Clause ATF-31.

17.0 ACCESS TO RECORDS, DATA AND FACILITIES. The contractor shall permit the CO and/or designated representative(s) access at any reasonable time to all records, data and facilities used in performance for the services covered in this SOW.

18.0 POINTS OF CONTACT

18.1. Contracting Points of Contract

The following ATF points of contacts have been established to assist in executing and administering the contract. All requests for interpretation and assistance should be referred to:

Bureau of ATF
James Huff, Contracting Officer (CO)
99 New York Avenue, NE, Washington, DC 20226
202-648-9117, James.Huff@atf.gov

Contracting Officer's Representative (COR): TBD

19.0 CONTRACT MANAGEMENT. Notwithstanding the contractor responsibility for total management responsibility during the performance of this contract, the administration of the contract will require maximum coordination between the Contracting Officer (CO), the Contracting Officer's Representative (COR) and the contractor. The following individuals will be the Government points of contact during performance of the contract:

(a) Contracting Officer (CO): The CO is responsible for the contract administration. The CO is the only person authorized to approve changes in the terms, conditions, delivery schedules, technical requirements or price, as set forth in the contract. Any changes not made expressly by the Contracting Office will be considered to have been without authority. In such cases, the Contractor is operating at their own risk.

No adjustment will be made in the contract price to cover any increase in charges incurred as a result thereof. The CO is James Huff. During any absence of the CO, identified for this contract, other warranted COs from ATF may authorize work under the contract.

(b) Contracting Officer's Representative (COR): A COR will be designated on authority of the CO to monitor all technical aspects and assist in administering the contract. The types of actions within the purview of the COR's authority are to assure that the Contractor performs the technical requirements of the contract; to perform, or cause to be performed, inspections necessary in connection with performance of the contract; to maintain both written and oral communications with the Contractor concerning the aspects of the contract within his/her purview; to monitor the Contractor's performance under the contract and notify the Contractor and CO of any deficiencies observed; and to coordinate Government furnished property availability and provide for site entry of Contractor personnel, if required.

20.0 OTHER CONTRACT REQUIREMENTS.

- a) The contractor shall be responsive to technical direction provided by the COR.
- b) The contractor must interact with technical personnel to support the goals and objectives of ATF and DOJ.
- c) The Contractor shall be responsible for the effective management of all training provided under this procurement.

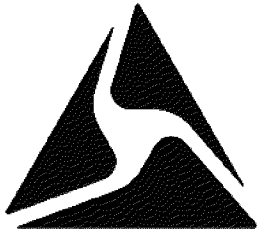
Attachment 2
Axon Quote with Price List and
Terms

Q-256699-44140.728JT

Issued: 11/03/2020

Quote Expiration: 12/11/2020

Account Number: 113182

Payment Terms: Net 30
Delivery Method: Fedex - Ground

Axon Enterprise, Inc.
17800 N 85th St.
Scottsdale, Arizona 85255
United States
Phone: (800) 978-2737

SHIP TO

Paul Vanderplow
BUREAU OF ALCOHOL TOBACCO &
FIREARMS - ATF HQ
99 NEW YORK AVENUE NE
7TH FLOOR EAST
WASHINGTON, DC 20226
US

BILL TO

BUREAU OF ALCOHOL TOBACCO &
FIREARMS - ATF HQ
99 NEW YORK AVENUE, NE,
WASHINGTON, DC 20226
US

SALES REPRESENTATIVE

(b) (6), (b) (7)(C)
Phone: (b) (6), (b) (7)(C)
Email: (b) (6), (b) (7)(C)
Fax:

PRIMARY CONTACT

Paul Vanderplow
Phone: (b) (6), (b) (7)(C)
Email:

Year 1

Item	Description	Term (Months)	Quantity	List Unit Price	Net Unit Price	Total (USD)
Axon Plans & Packages						
73683	10 GB EVIDENCE.COM A-LA-CART STORAGE	60	250,000			
Other						
73870	DEMS ONLY PROFESSIONAL EVIDENCE.COM ENTERPRISE LICENSE	60	1			
73871	DEMS ONLY CITIZEN FOR COMMUNITIES LICENSE	60	1			
73872	DEMS ONLY REDACTION ASSISTANT LICENSE	60	1			
73873	DEMS ONLY ADVANCE USER MANAGEMENT LICENSES	60	1			
73874	DEMS ONLY ADV DIGITAL EVIDENCE MANAGEMENT ADD-ON	60	1			
73875	DEMS ONLY AUTO TAGGING LICENSE		1			
73858	DIGITAL EVIDENCE MANAGEMENT BUNDLE PAYMENT 1001-5000	12	1			
Services						
85144	AXON STARTER		1			
80146	VIRTUAL BODYCAM STARTER		1			
85144	AXON STARTER		1			
80146	VIRTUAL BODYCAM STARTER		1			
80146	VIRTUAL BODYCAM STARTER		1			
80146	VIRTUAL BODYCAM STARTER		1			

(b) (4)

Year 2

Protect Life.

Year 3

Item	Description	Term (Months)	Quantity	List Unit Price	Net Unit Price	Total (USD)
Other						
73858	DIGITAL EVIDENCE MANAGEMENT BUNDLE PAYMENT 1001-5000	12	1	(b) (4) .00	(b) (4)	(b) (4)
Subtotal						(b) (4)
Estimated Tax						0.00
Total						(b) (4)

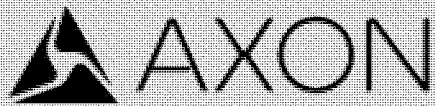
Year 4

Item	Description	Term (Months)	Quantity	List Unit Price	Net Unit Price	Total (USD)
Other						
73858	DIGITAL EVIDENCE MANAGEMENT BUNDLE PAYMENT 1001-5000	12	1	(b) (4) .00	(b) (4)	(b) (4)
Subtotal						(b) (4)
Estimated Tax						0.00
Total						(b) (4)

Year 5

Item	Description	Term (Months)	Quantity	List Unit Price	Net Unit Price	Total (USD)
Other						
73858	DIGITAL EVIDENCE MANAGEMENT BUNDLE PAYMENT 1001-5000	12	1	(b) (4) .00	(b) (4)	(b) (4)
Subtotal						(b) (4)
Estimated Tax						0.00
Total						(b) (4)

Grand Total	(b) (4)
-------------	---------



Discounts (USD)

Quote Expiration: 12/11/2020

List Amount		(b) (4)
Discounts		
Total		

**Total excludes applicable taxes*

Summary of Payments

Payment	Amount (USD)
Year 1	1,275,000.00
Year 2	(b) (4)
Year 3	(b) (4)
Year 4	(b) (4)
Year 5	(b) (4)
Grand Total	(b) (4)

Tax is subject to change at order processing with valid exemption.

Axon’s Sales Terms and Conditions

This Quote is limited to and conditional upon your acceptance of the provisions set forth herein and Axon's Master Services and Purchasing Agreement (posted at www.axon.com/legal/sales-terms-and-conditions), as well as the attached Statement of Work (SOW) for Axon Fleet and/or Axon Interview Room purchase, if applicable. Any purchase order issued in response to this Quote is subject solely to the above referenced terms and conditions. By signing below, you represent that you are lawfully able to enter into contracts. If you are signing on behalf of an entity (including but not limited to the company, municipality, or government agency for whom you work), you represent to Axon that you have legal authority to bind that entity. If you do not have this authority, please do not sign this Quote.

Signature:

Date:

Name (Print):

Title:

PO# (Or write N/A):

Please sign and email to Jesse Todd at jtodd@axon.com or fax to

Thank you for being a valued Axon customer. For your convenience on your next order, please check out our online store buy.axon.com

The trademarks referenced above are the property of their respective owners.

Axon Internal Use Only

		SFDC Contract #:
		Order Type:
		RMA #:
		Address Used:
		SO #:
Review 1	Review 2	
Comments:		





Axon Federal will honor the following 2020 Law Enforcement Agency Pricing toward incremental requirements, with a 10% discount off the Agency Price, through the execution of the base year and each option year exercised. Quantity requirements do not exist to receive the discount.

17800 N. 85th St. Scottsdale, AZ 85255-6311
 800.978.2737 Toll Free • 480.991.0791 Fax
 www.axon.com • Sales@axon.com

2020 Law Enforcement Agency Pricing – Axon Systems

Officer Safety Plan (OSP) Bundle/Payment

Model	Product Description	Agency Price
N/A	Officer Safety Plan 7 (OSP7)	(b) (4)
N/A	Officer Safety Plan 7 Plus (OSP7+)	

Axon Flex 2 Camera Hardware and Accessories

Model	Product Description
11528	Axon Flex 2 Camera (online)
11529	Axon Flex 2 Camera (offline)
11532	Axon Flex 2 Controller
11544	Oakley Flak Jacket Kit, Axon Flex 2
71037	Low Rider Headband, Axon Flex 2
11545	Collar Mount, Axon Flex 2
11554	Clip, Oakley, Axon Flex 2
11546	Epaulette Mount, Axon Flex 2
11547	Ballcap Mount, Axon Flex 2
11555	Mount, Ballistics Vest, Axon Flex 2
11548	Universal Helmet Mount, Axon Flex 2
11549	Tactical SWAT Kit with ARC Rail, Axon Flex 2
11533	Cable, Coiled, Straight to Right Angle, 48", Axon Flex 2
11534	USB Sync Cable, Axon Flex 2

Axon Body 2 Camera Hardware and Accessories

Model	Product Description
74001	Axon Body 2 Camera System (online)
74004	Axon Body 2 Camera System (offline)
74006	Axon Body 2 Battery Pack
11553	USB Sync Cable

Axon Body 2 Camera and Flex 2 Controller Mounts

Model	Product Description
74018	Z-Bracket, Men's, Axon RapidLock
74019	Z-Bracket, Women's Axon RapidLock
74020	Magnet, Flexible, Axon RapidLock
74021	Magnet, Outerwear, Axon RapidLock
74022	Small Pocket, 4" (10.1 cm), Axon RapidLock
74023	Large Pocket, 6" (15.2 cm), Axon RapidLock
71026	Reinforced Flexible Magnet Mount, Axon RapidLock
74028	Wing Clip Mount, Axon RapidLock
11507	MOLLE Mount, Single, Axon RapidLock
11508	MOLLE Mount, Double, Axon RapidLock
11509	Belt Clip Mount, Axon RapidLock

Axon Body 3 Camera Hardware and Accessories

Model	Product Description
73202	Axon Body 3 Camera System
74210	Axon Body 3 8-Bay Dock
74211	Axon Body 3 1-Bay Dock
N/A	Axon Aware
N/A	Axon Aware Plus

Title: 2020 Axon Law Enforcement Agency Pricing
 Department: Sales & Customer Service
 Version: 1.0
 Release Date: 4/9/2020

**Axon Signal Hardware & Services**

Model	Product Description	Agency Price
70112	Axon Signal Vehicle unit (1 per car/motor)	(b) (4)
80129	Axon Signal Vehicle unit installation and/or training	
70116	Axon Signal Performance Power Magazine (SPPM)	
75000	Axon Signal Sidearm Adhesive Mount	

Axon Fleet 2 Package

Model	Product Description
N/A	Axon Fleet 2 Unlimited Package with TASER Assurance Plan (TAP). PER VEHICLE: Includes all required hardware, 5-year Technology Assurance Plan, unlimited Axon Evidence (Evidence.com) storage (for that vehicle), and one View XL application license. DOES NOT INCLUDE routers, Axon Evidence user licenses, wireless offload servers, wireless offload infrastructure, or installation costs.
N/A	Axon Fleet 2 Unlimited Package <i>without</i> TASER Assurance Plan (TAP). PER VEHICLE: Includes all required hardware, 5-year Technology Assurance Plan, unlimited Axon Evidence (Evidence.com) storage (for that vehicle), and one View XL application license. DOES NOT INCLUDE routers, Axon Evidence user licenses, wireless offload servers, wireless offload infrastructure, or installation costs.

Axon Fleet 2 Cradlepoint Router Bundle (per vehicle, for Wi-Fi offload)

Model	Product Description
11634	Cradlepoint Router IBR900-1200M-NPS, NetCloud + CradleCare Service Package
11511	Axon Fleet 2 Router Antenna
74110	Cable, CAT6 Ethernet 25 Ft

Axon Fleet 2 Wireless Offload Servers & Installation (varies by location)

Model	Product Description
74074	Wi-Fi Offload Server Hardware
	Wi-Fi Offload Software License

Axon Fleet 2 Installation & Professional Services

Model	Product Description
74063	Standard Axon Fleet Installation (Per Vehicle)

Axon Interview Room

Model	Product Description
50114	Axis Sensor Unit F1025
74059	Motion Sensor Enclosure – Covert Camera
74055	Fire Strobe - Red
50281	Axis Camera, Axis Q3515-LV Network Camera
50118	Louroe Microphone (POE)
50123	HP Switch – 8 port Gigabit Max POE Managed Switch
50124	HP Switch – 24 port Gigabit Max POE Managed Switch
50144	Recording Server – Windows 2012 R2 64 bit – 2U Xeon (4-core)
50206	Recording Server Lite, 1U Rack Server, Xeon (4-Core), 8GB ME
74056	Touch Panel Wall Mount
85170	Interview Room, Install and Setup (one day)
74062	Interview Room 5 yr Extended Warranty
50074	Axon Touch Panel Software Maintenance Annual Payment

Axon Dock Hardware

Model	Product Description
11536	1-bay + Core Axon Dock for Axon Flex 2
11537	6-bay + Core Axon Dock for Axon Flex 2
11538	1-bay for Axon Flex 2

**Axon Dock Hardware**

Model	Product Description	Agency Price
11539	6-bay for Axon Flex 2	(b) (4)
74009	1-bay + Core Axon Dock for Axon Body 2	
74008	6-bay + Core Axon Dock for Axon Body 2	
74011	1-bay for Axon Body 2	
74010	6-bay for Axon Body 2	
70027	Axon Dock Core, compatible with all 1-bays and 6-bays	
70033	Wall mount, Axon Dock	
70040	Desk plate, Axon Dock	

Customer Care Extended Warranty

Model	Product Description
N/A	Tech Assurance Plan 1-Bay Axon Body 2 Dock Warranty*
N/A	Tech Assurance Plan 6-Bay Axon Body 2 Dock Warranty*
N/A	Tech Assurance Plan 1-Bay Axon Flex 2 Dock Warranty*
N/A	Tech Assurance Plan 6-Bay Axon Flex 2 Dock Warranty*
N/A	Tech Assurance Plan 1-Bay Axon Body 3 Dock Warranty*
N/A	Tech Assurance Plan Axon Body 2 Camera Warranty*
N/A	Tech Assurance Plan Axon Flex 2 Camera and Controller Warranty*
N/A	Axon Body 3 Camera TAP Warranty*
N/A	Axon Body 3 Camera 8-Bay Dock TAP Warranty*

*Minimum 30 month purchase required per refresh.

Axon Evidence (Evidence.com) Services

Model	Product Description
N/A	Axon Performance License
N/A	Evidence.com Basic License
N/A	Pro Evidence.com License
N/A	10 GB Evidence.com A-La-Carte Storage
N/A	10 GB Evidence.com Archival Storage
80190	Axon Evidence Channel Services Fee
80191	Axon Evidence Channel Migration, TB Annual
80230	Axon Evidence Channel SMA Annual
N/A	Auto Tagging License

Axon Professional Services

Model	Product Description
80146	Virtual Body Worn Camera Starter Service
85055	Axon Full Service
85144	Axon Starter
85146	Axon 1-Day Service

Axon may change pricing or product offerings at any point in time. The committed pricing is based on each Axon Quote provided to the Agency.

All taxes, duties and customs, where applicable, are the responsibilities of the customer.

Pricing Pricing for Law Enforcement/Correctional Agencies Only. Must be a sworn law enforcement officer to purchase.

ALL SALES ARE FINAL.

For delivery status or information on how to place an order, call our sales department at 800-978-2737, fax: 480-991-0791

Axon Enterprise, Inc.'s Sales Terms and Conditions for Direct Sales to End User Purchasers apply to all sales and are available at <http://www.axon.com/sales-terms-and-conditions>.



Axon ATF Terms

1 **Definitions.**

"Axon Cloud Services" means Axon's web services for Axon Evidence, Axon Records, Axon Dispatch, and interactions between Evidence.com and Axon Devices or Axon client software. Axon Cloud Service excludes third-party applications, hardware warranties, and my.evidence.com.

"Axon Devices" means all hardware provided by Axon under the SOW.

"Services" means all services provided by Axon under the Agreement, including software, Axon Cloud Services, and professional services.

2 **Returns.** All sales are final. Axon does not allow refunds or exchanges, except warranty returns or as provided by state or federal law. Agency will notify Axon of any defective Axon Devices within 7 days of receipt, or such Axon Devices will be deemed accepted.

3 **Warranty.**

3.1 Hardware Limited Warranty. Axon warrants that Axon-manufactured Devices are free from defects in workmanship and materials for 1 year from the date of Agency's receipt, except Signal Sidearm, which Axon warrants for 30 months from the date of Agency's receipt. Axon warrants its Axon-manufactured accessories for 90-days from the date of Agency's receipt. Used conducted energy weapon ("**CEW**") cartridges are deemed to have operated properly. Extended warranties run from the expiration of the 1-year hardware warranty through the extended warranty term. Non-Axon manufactured Devices are not covered by Axon's warranty. Agency should contact the manufacturer for support of non-Axon manufactured Devices.

3.2 Claims. If Axon receives a valid warranty claim for an Axon manufactured Device during the warranty term, Axon's sole responsibility is to repair or replace the Device with the same or like Device, at Axon's option. A replacement Device will be new or like new. Axon will warrant the replacement Device for the longer of (a) the remaining warranty of the original Device or (b) 90-days from the date of repair or replacement.

If Agency exchanges a device or part, the replacement item becomes Agency's property, and the replaced item becomes Axon's property. Before delivering a Device for service, Agency must upload Device data to Axon Evidence or download it and retain a copy. Axon is not responsible for any loss of software, data, or other information contained in storage media or any part of the Device sent to Axon for service.

3.3 Spare Devices. Axon may provide Agency a predetermined number of spare Devices as detailed in the Quote ("**Spare Devices**"). Spare Devices will replace broken or non-functioning units. If Agency utilizes a Spare Device, Agency must return to Axon, through Axon's warranty return process, any broken or non-functioning units. Axon will repair or replace the unit with a replacement Device. Upon termination, Axon will invoice Agency the MSRP then in effect for all Spare Devices provided. If Agency returns the Spare Devices to Axon within 30 days of the invoice date, Axon will issue a credit and apply it against the invoice.

3.4 Limitations. Axon's warranty excludes damage related to: (a) failure to follow Device use instructions; (b) Devices used with equipment not manufactured or recommended by Axon; (c) abuse, misuse, or intentional damage to Device; (d) force majeure; (e) Devices repaired or modified by persons other than Axon without Axon's written permission; or (f) Devices with a defaced or removed serial number.

3.4.1 To the extent permitted by law, the above warranties and remedies are exclusive. Axon disclaims all other warranties, remedies, and conditions, whether oral, written, statutory, or implied. If statutory or implied warranties cannot be lawfully disclaimed, then such warranties are limited to the



Axon ATF Terms

duration of the warranty described above and by the provisions in the Agreement.

- 3.4.2 Axon's cumulative liability to any Party for any loss or damage resulting from any claim, demand, or action arising out of or relating to any Axon Device or Service will not exceed the purchase price paid to Axon for the Device, or if for Services, the amount paid for such Services over the 12 months preceding the claim. Neither Party will be liable for direct, special, indirect, incidental, punitive or consequential damages, however caused, whether for breach of warranty or contract, negligence, strict liability, tort or any other legal theory.

- 4 **IP Indemnification**. Axon will indemnify Agency Indemnitees against all claims, losses, and reasonable expenses from any third-party claim alleging that the use of Axon Devices or Services infringes or misappropriates the third-party's intellectual property rights. Agency must promptly provide Axon with written notice of such claim, tender to Axon the defense or settlement of such claim at Axon's expense and cooperate fully with Axon in the defense or settlement of such claim. Axon's IP indemnification obligations do not apply to claims based on (a) modification of Axon Devices or Services by Agency or a third-party not approved by Axon; (b) use of Axon Devices and Services in combination with hardware or services not approved by Axon; (c) use of Axon Devices and Services other than as permitted in this Agreement; or (d) use of Axon software that is not the most current release provided by Axon.
- 5 **Agency Responsibilities**. Agency is responsible for (a) Agency's use of Axon Devices; (b) breach of the Agreement or violation of applicable law by Agency or an Agency end user; and (c) a dispute between Agency and a third-party over Agency's policy regarding use of Axon Devices.
- 6 **Effect of Termination**. Upon termination of the Agreement, Agency rights immediately terminate. Agency remains responsible for all fees incurred before the effective date of termination. If Agency purchases Devices for less than the manufacturer's suggested retail price ("**MSRP**") and the Agreement terminates before the end of the Term, Axon will invoice Agency the difference between the MSRP for Devices received and amounts paid towards those Devices. If terminating for non-appropriation, Agency may return Devices to Axon within 30 days of termination. MSRP is the standalone price of the individual Device at the time of sale. For bundled Devices, MSRP is the standalone price of all individual components.



Axon ATF Terms

Axon Cloud Services Appendix

1 **Definitions.**

“Agency Content” is data uploaded into, ingested by, or created in Axon Cloud Services within Agency’s tenant, including media or multimedia uploaded into Axon Cloud Services by Agency. Agency Content includes Evidence but excludes Non-Content Data.

“Evidence” is media or multimedia uploaded into Axon Evidence as 'evidence' by an Agency. Evidence is a subset of Agency Content.

“Non-Content Data” is data, configuration, and usage information about Agency’s Axon Cloud Services tenant, Axon Devices and client software, and users that is transmitted or generated when using Axon Devices. Non-Content Data includes data about users captured during account management and customer support activities. Non-Content Data does not include Agency Content.

2 **Subscription Term.** For Axon Evidence subscriptions, including Fleet 2 Unlimited, the subscription begins after shipment of the applicable Axon Device. If Axon ships the Device in the first half of the month, the start date is the 1st of the following month. If Axon ships the Device in the second half of the month, the start date is the 15th of the following month. For phased deployments, the start date begins on shipment of phase one. For purchases solely of Axon Evidence subscriptions, the start date is the Effective Date. The Axon Evidence subscription term ends upon completion of the Axon Evidence subscription stated in the Quote (**“Axon Evidence Subscription Term”**). Start dates for Axon Records and Axon Dispatch will be addressed through an SOW.

3 **Access.** Upon Axon granting Agency a subscription to Axon Cloud Services, Agency may access and use Axon Cloud Services to store and manage Agency Content. Agency may not exceed more end users than the Quote specifies. Axon Air requires an Axon Evidence subscription for each drone operator. For Axon Evidence Lite, Agency may access and use Axon Evidence only to store and manage TASER CEW and TASER CAM data (**“TASER Data”**). Agency may not upload non-TASER Data to Axon Evidence Lite.

4 **Agency Owns Agency Content.** Agency controls and owns all right, title, and interest in Agency Content. Except as outlined herein, Axon obtains no interest in Agency Content, and Agency Content are not business records of Axon. Agency is solely responsible for uploading, sharing, managing, and deleting Agency Content. Axon will have limited access to Agency Content solely for providing and supporting Axon Cloud Services to Agency and Agency end users.

5 **Security.** Axon will implement commercially reasonable and appropriate measures to secure Agency Content against accidental or unlawful loss, access or disclosure. Axon will maintain a comprehensive information security program to protect Axon Cloud Services and Agency Content including logical, physical access, vulnerability, risk, and configuration management; incident monitoring and response; encryption of uploaded digital evidence; security education; and data protection. Axon agrees to the Federal Bureau of Investigation Criminal Justice Information Services Security Addendum.

6 **Agency Responsibilities.** Agency is responsible for (a) ensuring Agency owns Agency Content; (b) ensuring no Agency Content or Agency end user’s use of Agency Content or Axon Cloud Services violates this Agreement or applicable laws; and (c) maintaining necessary computer equipment and Internet connections for use of Axon Cloud Services. If Agency becomes aware of any violation of this Agreement by an end user, Agency will immediately terminate that end user’s access to Axon Cloud Services.

Agency will also maintain the security of end user names and passwords and security and access by end users to Agency Content. Agency is responsible for ensuring the configuration and utilization of Axon Cloud Services meet applicable Agency regulation and standards. Agency may not sell,



Axon ATF Terms

transfer, or sublicense access to any other entity or person. Agency shall contact Axon immediately if an unauthorized party may be using Agency's account or Agency Content, or if account information is lost or stolen.

- 7** **Privacy.** Axon will not disclose Agency Content or information about Agency except as compelled by a court or administrative body or required by law or regulation. If Axon receives a disclosure request for Agency Content, Axon will give Agency notice, unless legally prohibited from doing so, to allow Agency to file an objection with the court or administrative body. Agency agrees to allow Axon access to certain information from Agency to (a) perform troubleshooting services upon request or as part of regular diagnostic screening; (b) enforce this Agreement or policies governing the use of Axon Evidence; or (c) perform analytic and diagnostic evaluations of the systems.
- 8** **Storage.** For Axon Evidence Unlimited, Agency may store unlimited data in Agency's Axon Evidence account only if data originates from Axon Capture or an Axon body-worn camera. For Axon Air Evidence subscriptions, Agency may store unlimited data in Agency's Axon Evidence account only if data originates from an Axon Air device. For Axon Interview Room Unlimited, Agency may store unlimited data in Agency's Axon Evidence account only if data originates from Axon Interview Room hardware. For Axon Fleet Unlimited, Agency may store unlimited data in Agency's Axon Evidence account only if data originates from Axon Fleet hardware.

For us of an Unlimited Investigator license, the limits of such license are as follows:

Product Tier Name	Description	Storage Size
Unlimited Investigator Upload (1/2 Mbps)	Axon Investigator unlimited rate for upload of video/audio upload at 1/2 Mbps	164 GB / Month
Unlimited Investigator Upload (1 Mbps)	Axon Investigator unlimited rate for upload of video/audio upload at 1 Mbps	328 GB / Month
Unlimited Investigator Upload (2 Mbps)	Axon Investigator unlimited rate for upload of video/Audio at 2 Mbps	657 GB / Month
Unlimited Investigator Upload (4 Mbps)	Axon Investigator unlimited rate for upload of video/audio at 4 Mbps	1,314 GB / Month

Axon may charge Agency additional fees for exceeding purchased storage amounts. Since Agency is purchasing unlimited body-worn camera and Axon Capture storage, Agency will only be charged additional fees if Agency elects to store third-party content not originating from an Axon body-worn camera or Axon Capture within Agency's Axon Evidence tenant. Axon may place Agency Content that Agency has not viewed or accessed for 6 months into archival storage. Agency Content in archival storage will not have immediate availability and may take up to 24 hours to access.

- 9** **Location of Storage.** Axon may transfer Agency Content to third-party subcontractors for storage. Axon will determine the locations of data centers for storage of Agency Content. For United States agencies, Axon will ensure all Agency Content stored in Axon Cloud Services remains within the United States. Ownership of Agency Content remains with Agency.
- 10** **Suspension.** Axon may temporarily suspend Agency's or any end user's right to access or use any portion or all of Axon Cloud Services immediately upon notice, if Agency or end user's use of or registration for Axon Cloud Services may (a) pose a security risk to Axon Cloud Services or any third-party; (b) adversely impact Axon Cloud Services, the systems, or content of any other customer; (c) subject Axon, Axon's affiliates, or any third-party to liability; or (d) be fraudulent.



Axon ATF Terms

-
- Agency remains responsible for all fees incurred through suspension. Axon will not delete Agency Content because of suspension, except as specified in this Agreement.
- 11 **Axon Cloud Services Warranty.** Axon disclaims any warranties or responsibility for data corruption or errors before Agency uploads data to Axon Cloud Services.
 - 12 **Axon Cloud Services Restrictions.** Agency and Agency end users (including employees, contractors, agents, officers, volunteers, and directors), may not, or may not attempt to:
 - 12.1. copy, modify, tamper with, repair, or create derivative works of any part of Axon Cloud Services;
 - 12.2. reverse engineer, disassemble, or decompile Axon Cloud Services or apply any process to derive any source code included in Axon Cloud Services, or allow others to do the same;
 - 12.3. access or use Axon Cloud Services with the intent to gain unauthorized access, avoid incurring fees or exceeding usage limits or quotas;
 - 12.4. use trade secret information contained in Axon Cloud Services, except as expressly permitted in this Agreement;
 - 12.5. access Axon Cloud Services to build a competitive device or service or copy any features, functions, or graphics of Axon Cloud Services;
 - 12.6. remove, alter, or obscure any confidentiality or proprietary rights notices (including copyright and trademark notices) of Axon's or Axon's licensors on or within Axon Cloud Services; or
 - 12.7. use Axon Cloud Services to store or transmit infringing, libelous, or other unlawful or tortious material; to store or transmit material in violation of third-party privacy rights; or to store or transmit malicious code.
 - 13 **After Termination.** Axon will not delete Agency Content for 90-days following termination. There will be no functionality of Axon Cloud Services during these 90-days other than the ability to retrieve Agency Content. Agency will not incur additional fees if Agency downloads Agency Content from Axon Cloud Services during this time. Axon has no obligation to maintain or provide Agency Content after these 90-days and will thereafter, unless legally prohibited, delete all Agency Content. Upon request, Axon will provide written proof that Axon successfully deleted and fully removed all Agency Content from Axon Cloud Services.
 - 14 **Post-Termination Assistance.** Axon will provide Agency with the same post-termination data retrieval assistance that Axon generally makes available to all customers. Requests for Axon to provide additional assistance in downloading or transferring Agency Content, including requests for Axon's data egress service, will result in additional fees and Axon will not warrant or guarantee data integrity or readability in the external system.
 - 15 **U.S. Government Rights.** If Agency is a U.S. Federal department or using Axon Cloud Services on behalf of a U.S. Federal department, Axon Cloud Services is provided as a "commercial item," "commercial computer software," "commercial computer software documentation," and "technical data", as defined in the Federal Acquisition Regulation and Defense Federal Acquisition Regulation Supplement. If Agency is using Axon Cloud Services on behalf of the U.S. Government and these terms fail to meet the U.S. Government's needs or are inconsistent in any respect with federal law, Agency will immediately discontinue use of Axon Cloud Services.
 - 16 **Survival.** Upon any termination of this Agreement, the following sections in this Appendix will survive: Agency Owns Agency Content, Storage, Axon Cloud Services Warranty, and Axon Cloud Services Restrictions.
-



Axon ATF Terms

Professional Services Appendix

- 1 **Utilization of Services.** Agency must use pre-paid professional services as outlined in the Quote and this Appendix within 6 months of the Effective Date.
- 2 **Body-Worn Camera Full Service (BWC Full Service).** BWC Full Service includes 4 consecutive days of on-site service and a professional services manager to work with Agency to assess Agency's deployment and determine which on-site services are appropriate. If Agency requires more than 4 consecutive on-site days, additional days are \$2,500 per day. BWC Full Service options include:

System set up and configuration

- Setup Axon View on smartphones (if applicable)
- Configure categories and custom roles based on Agency need
- Register cameras to Agency domain
- Troubleshoot IT issues with Axon Evidence and Axon Dock ("Dock") access
- One on-site session included

Dock configuration

- Work with Agency to decide the ideal location of Docks and set configurations on Dock
- Authenticate Dock with Axon Evidence using admin credentials from Agency
- On-site assistance, not to include physical mounting of docks

Best practice implementation planning session

- Provide considerations for the establishment of video policy and system operations best practices based on Axon's observations with other agencies
- Discuss the importance of entering metadata in the field for organization purposes and other best practice for digital data management
- Provide referrals of other agencies using the Axon camera devices and Axon Evidence
- Recommend rollout plan based on review of shift schedules

System Admin and troubleshooting training sessions

Step-by-step explanation and assistance for Agency's configuration of security, roles & permissions, categories & retention, and other specific settings for Axon Evidence

Axon instructor training (Train the Trainer)

Training for Agency's in-house instructors who can support Agency's Axon camera and Axon Evidence training needs after Axon has fulfilled its contractual on-site obligations

Evidence sharing training

Tailored workflow instruction for Investigative Units on sharing Cases and Evidence with local prosecuting agencies

End user go-live training and support sessions

- Assistance with device set up and configuration
- Training on device use, Axon Evidence, and Evidence Sync

Implementation document packet

Axon Evidence administrator guides, camera implementation guides, network setup guide, sample policies, and categories & roles guide

Post go-live review

- 3 **Body-Worn Camera 1-Day Service (BWC 1-Day).** BWC 1-Day includes one day of on-site Services and a professional services manager to work closely with Agency to assess Agency's deployment and determine which Services are appropriate. If Agency requires more than 1 day of on-site Services, additional on-site assistance is \$2,500 per day. The BWC 1-Day options include:



Axon ATF Terms

System set up and configuration (Remote Support)

- Setup Axon Mobile on smartphones (if applicable)
- Configure categories & custom roles based on Agency need
- Troubleshoot IT issues with Axon Evidence and Axon Dock (“**Dock**”) access

Dock configuration

- Work with Agency to decide the ideal location of Dock setup and set configurations on Dock
- Authenticate Dock with Axon Evidence using “Administrator” credentials from Agency
- Does not include physical mounting of docks

Axon instructor training (Train the Trainer)

Training for Agency’s in-house instructors who can support Agency’s Axon camera and Axon Evidence training needs after Axon’s has fulfilled its contracted on-site obligations

End user go-live training and support sessions

- Assistance with device set up and configuration
- Training on device use, Axon Evidence, and Evidence Sync

Implementation document packet

Axon Evidence administrator guides, camera implementation guides, network setup guide, sample policies, and categories & roles guide

- 4** **Body-Worn Camera Virtual 1-Day Service (BWC Virtual).** BWC Virtual includes all items in the BWC 1-Day Service Package, except one day of on-site services.
- 5** **Out of Scope Services.** Axon is only responsible to perform the professional services described in the Quote and this Appendix. Any additional professional services are out of scope. The Parties must document scope changes in a written and signed change order. Changes may require an equitable adjustment in the charges or schedule.
- 6** **Delivery of Services.** Axon personnel will work Monday through Friday, 8:30 a.m. to 5:30 p.m., except holidays. Axon will perform all on-site tasks over a consecutive timeframe. Axon will not charge Agency travel time by Axon personnel to Agency premises as work hours.
- 7** **Access Computer Systems to Perform Services.** Agency authorizes Axon to access relevant Agency computers and networks, solely for performing the Services. Axon will work to identify as soon as reasonably practicable resources and information Axon expects to use and will provide an initial itemized list to Agency. Agency is responsible for and assumes the risk of any problems, delays, losses, claims, or expenses resulting from the content, accuracy, completeness, and consistency of all data, materials, and information supplied by Agency.
- 8** **Site Preparation.** Axon will provide a hardcopy or digital copy of current user documentation for the Devices (“**User Documentation**”). User Documentation will include all required environmental specifications for the professional Services and Devices to operate per the Device User Documentation. Before installation of Devices (whether performed by Agency or Axon), Agency must prepare the location(s) where Devices are to be installed (“**Installation Site**”) per the environmental specifications in the Device User Documentation. Following installation, Agency must maintain the Installation Site per the environmental specifications. If Axon modifies Device User Documentation for any Devices under this Agreement, Axon will provide the update to Agency when Axon generally releases it.
- 9** **Acceptance.** When Axon completes professional Services, Axon will present an acceptance form (“**Acceptance Form**”) to Agency. Agency will sign the Acceptance Form acknowledging completion. If Agency reasonably believes Axon did not complete the professional Services in substantial conformance with this Agreement, Agency must notify Axon in writing of the specific



Axon ATF Terms

reasons for rejection within 7 calendar days from delivery of the Acceptance Form. Axon will address the issues and re-present the Acceptance Form for signature. If Axon does not receive the signed Acceptance Form or written notification of reasons for rejection within 7 calendar days of delivery of the Acceptance Form, Axon will deem Agency to have accepted the professional Services.

- 10** **Agency Network.** For work performed by Axon transiting or making use of Agency's network, Agency is solely responsible for maintenance and functionality of the network. In no event will Axon be liable for loss, damage, or corruption of Agency's network from any cause.



Axon ATF Terms

Advanced User Management Appendix

- 1 **Scope.** Advanced User Management allows Agency to (a) utilize bulk user creation and management, (b) automate user creation and management through System for Cross-domain Identity Management (“**SCIM**”), and (c) automate group creation and management through SCIM.
- 2 **Pricing.** Agency must purchase Advanced User Management for every Axon Evidence user in Agency, even if the user does not have an Axon body camera.
- 3 **Advanced User Management Configuration.** Agency will work independently to configure Agency's Advanced User Management for Agency's applicable Use. Upon request, Axon will provide general guidance to Agency, including documentation that details the setup and configuration process.

To: Vanderplow, Paul D[(b) (6), (b) (7)(C)]
From: [(b) (6), (b) (7)(C)]
Sent: Wed 8/11/2021 3:36:22 PM
Subject: ATF BWC Phase I Announcement

It is lengthy but I'm not sure how familiar the DAD's are with the background, edit as you deem necessary.

(b) (5)

[(b) (6), (b) (7)(C)]
Alcohol, Tobacco, Firearms and Explosives
16009 N. 81st Street, Suite 100
Scottsdale, AZ 85260

Special Agent Project Officer-Digital Evidence Management
Technical Project Office
Special Operations Division
(b) (6), (b) (7)(C)

CONFIDENTIALITY NOTICE: E-mail may contain confidential information that is legally privileged. Do not read this e-mail if you are not the intended recipient.

This e-mail transmission, and any documents, files or previous e-mail messages attached to it may contain confidential information that is legally privileged. If you are not the intended recipient, or a person responsible for delivering it to the intended recipient, you are hereby notified that any disclosure, copying, distribution or use of any of the information contained in or attached to this transmission is **STRICTLY PROHIBITED**. If you have received this transmission in error, please immediately notify us by reply e-mail, by forwarding this to (b) (6), (b) (7)(C) or by telephone at (b) (6), (b) (7)(C) and destroy the original transmission and its attachments without reading or saving in any manner. Thank you.

To: Braverman, Adam L. (ODAG)(b) (6), (b) (7)(C)]
Cc: Vanderplow, Paul D.(b) (6), (b) (7)(C)
From: (b) (6), (b) (7)(C)
Sent: Thur 7/22/2021 6:29:38 PM
Subject: Revised ATF BWC Policy
ATF Policy BWC 7_22_21.docx

Sir,

Based on our discussion last week and your subsequent conversation with Chief Vanderplow yesterday, we have made some revisions to ATF's BWC Policy for your review.

(b) (6), (b) (7)(C)
Alcohol, Tobacco, Firearms and Explosives
16009 N. 81st Street, Suite 100
Scottsdale, AZ 85260
Special Agent Project Officer-Digital Evidence Management
Technical Project Office
Special Operations Division
(b) (6), (b) (7)(C)

CONFIDENTIALITY NOTICE: E-mail may contain confidential information that is legally privileged. Do not read this e-mail if you are not the intended recipient.

This e-mail transmission, and any documents, files or previous e-mail messages attached to it may contain confidential information that is legally privileged. If you are not the intended recipient, or a person responsible for delivering it to the intended recipient, you are hereby notified that any disclosure, copying, distribution or use of any of the information contained in or attached to this transmission is **STRICTLY PROHIBITED**. If you have received this transmission in error, please immediately notify us by reply e-mail, by forwarding this to (b) (6), (b) (7)(C) or by telephone at (b) (6), (b) (7)(C) and destroy the original transmission and its attachments without reading or saving in any manner. Thank you.

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

To: (b) (6), (b) (7)(C)
Cc: Vanderplow, Paul D[(b) (6), (b) (7)(C)
From: (b) (6), (b) (7)(C)
Sent: Fri 8/20/2021 5:38:01 PM
Subject: Body-worn camera

Ma'am,

June 7, 2021, The Deputy Attorney General (DAG) has mandated all DOJ components to implement a phase I body-worn camera (BWC) program. ATF is scheduled to begin phase I on September 1, 2021. Phase I of body-worn camera implementation will include and require special agents in the Phoenix Field Division, Detroit Field Division, and the ATF National academy to wear body-worn cameras during pre-planned arrest warrants and pre-planned search warrants.

(b) (5)

Please respond if this is acceptable or what is acceptable to your directorate. Thank you and apologies for the quick turnaround request.

(b) (6), (b) (7)(C)
Alcohol, Tobacco, Firearms and Explosives
16009 N. 81st Street, Suite 100
Scottsdale, AZ 85260
Special Agent Project Officer-Digital Evidence Management
Technical Project Office
Special Operations Division
(b) (6), (b) (7)(C)

CONFIDENTIALITY NOTICE: E-mail may contain confidential information that is legally privileged. Do not read this e-mail if you are not the intended recipient.

This e-mail transmission, and any documents, files or previous e-mail messages attached to it may contain confidential information that is legally privileged. If you are not the intended recipient, or a person responsible for delivering it to the intended recipient, you are hereby notified that any disclosure, copying, distribution or use of any of the information contained in or attached to this transmission is **STRICTLY PROHIBITED**. If you have received this transmission in error, please immediately notify us by reply e-mail, by forwarding this to (b) (6), (b) (7)(C) or by telephone at (b) (6), (b) (7)(C) and destroy the original transmission and its attachments without reading or saving in any manner. Thank you.

To: (b) (6), (b) (7)(C)
From: (b) (6), (b) (7)(C)
Sent: Wed 6/30/2021 4:22:56 PM
Subject: FW: New Mexico TFO MOU
DOC012.pdf
ATF BWC-TFO Checklist 12_04_2020.pdf

Visual Labs is the name of the BWC vendor...

(b) (6), (b) (7)(C)
Alcohol, Tobacco, Firearms and Explosives
16009 N. 81st Street, Suite 100
Scottsdale, AZ 85260
Special Agent Project Officer-Digital Evidence Management
Technical Project Office
Special Operations Division
(b) (6), (b) (7)(C)

CONFIDENTIALITY NOTICE: E-mail may contain confidential information that is legally privileged. Do not read this e-mail if you are not the intended recipient.

This e-mail transmission, and any documents, files or previous e-mail messages attached to it may contain confidential information that is legally privileged. If you are not the intended recipient, or a person responsible for delivering it to the intended recipient, you are hereby notified that any disclosure, copying, distribution or use of any of the information contained in or attached to this transmission is **STRICTLY PROHIBITED**. If you have received this transmission in error, please immediately notify us by reply e-mail, by forwarding this to (b) (6), (b) (7)(C) or by telephone at (b) (6), (b) (7)(C) and destroy the original transmission and its attachments without reading or saving in any manner. Thank you.

From: (b) (6), (b) (7)(C)
Sent: Tuesday, June 29, 2021 12:30 PM
To: (b) (6), (b) (7)(C)
Subject: New Mexico TFO MOU

Hello (b) (6), (b) (7)(C) the one sheriff's office that you were on standby for a few weeks ago has returned the BWC docs. Could you take a look at them please? A couple things I noticed on the Addendum:

(b) (5)

Thank you,

(b) (6), (b) (7)(C)

Addendum to Task Force Agreements Pertaining to Body Worn Cameras

This addendum supplements the agreement between the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and the Valencia County Sheriff's Office dated June 22, 2021, establishing the Albuquerque Group I Task Force Pursuant to the "Department of Justice Policy – Use of Body-Worn Cameras (BWC) by Federally Deputized Task Force Officers," dated June 22, 2021. Valencia County Sheriff's Office has advised ATF that it will require its deputized officers participating in the Task Force to use Body Worn Cameras (BWCs). This addendum governs that use.

The parties hereby agree to the following:

- I. TFOs will adhere to the DOJ Policy, ATF's Standard Operating Procedures for Task Force Officer Body Camera Program, and other applicable ATF policies and procedures.
- II. Valencia County Sheriff's Office confirms that prior to executing this agreement it has provided to ATF details regarding the BWC system and cameras, including the details of any system protections, and any state or local policies or laws applicable to the TFO's use of BWCs, including any retention policies as detailed in Attachment 1 – Agency Checklist.
- III. Use of BWCs During Federal Task Force Operations:
 - A. Deputized Task Force Officers (TFO) through the Joint Law Enforcement Operations (JLEO) Program will be allowed to wear and activate their recording equipment with BWCs for the purposes of recording their actions only during:
 1. A planned attempt to serve an arrest warrant or other planned arrest; or
 2. The execution of a search warrant.
 - B. TFOs are authorized to activate their BWCs upon making entry into a premises or upon approaching a subject, and must deactivate their BWCs when the scene is secured as determined by the federal supervisor on the scene as designated by the sponsoring federal agency.
 1. For purposes of this agreement, the term "secured" means that the scene is safe and under law enforcement control.
 2. In the event circumstances arise requiring additional law enforcement assistance to secure the scene, the TFO will end BWC recording when relieved from the scene by another law enforcement agency.
 3. For the execution of a search warrant, BWCs should not be used for searches of property lawfully in government custody or control, or a search to obtain digital or electronic records executed by a third party, such as an electronic service provider or custodian of electronic records.

Addendum to Task Force Agreements Pertaining to Body Worn Cameras

- C. TFOs will follow the provisions set forth in this agreement for use of BWCs, and the provisions of this agreement will supersede any conflicting provision in the agency's policy for TFOs while serving on the federal Task Force.
- D. TFOs may use BWCs in accordance with this policy anywhere they are authorized to act as a police or peace officer under state, local, territorial or tribal law.
- E. TFOs may use only agency-issued and agency-owned BWCs. TFOs will not be allowed to possess or use any privately owned BWC or other recording device of any kind.
- F. In the event a TFO's BWC is not working or inoperable due to a technical problem or cannot be used due to physical damage, and, in the judgement of the Task Force supervisor, delaying the operation to repair or obtain a replacement BWC is not practical or would impair the operation, the TFO may participate in the operation without using a BWC.
- G. Even when BWC use would be permissible in the circumstances set forth in Section III A above, TFOs are prohibited from recording:
 - 1. Undercover personnel;
 - 2. Confidential informants or confidential sources;
 - 3. On-scene witness interviews prior to or after the operation;
 - 4. Personnel using specialized investigative techniques or equipment; or
 - 5. Actions by any non-law enforcement persons at the scene who are assisting law enforcement personnel.
- H. Even when BWC use would be permissible in the circumstances set forth above in Section III A above, TFOs are prohibited from activating their BWC if, in the judgement of the ATF, the TFO:
 - 1. National Security (including international and domestic terrorism investigations or cases involving classified information);
 - 2. Public Corruption;
 - 3. Medical Facilities; or
 - 4. Other sensitive investigations as determined by ATF.
- I. Even when BWC use would be permissible in the circumstances set forth in Section III A above, TFOs shall not use BWCs to record any activities related to:
 - 1. Is using specialized or sensitive investigative techniques;
 - 2. Is operating in a sensitive area; or
 - 3. Is working in an undercover or covert status on behalf of the federal task force.

Addendum to Task Force Agreements Pertaining to Body Worn Cameras

IV. Valencia County Sheriff's Office Internal Controls:

- A. Undersheriff Jeff Noah will serve as a point-of-contact (POC) for ATF on BWC matters.
- B. Valencia County Sheriff's Office will notify ATF of any change in state or local law that will modify how ATF TFOs must use BWCs or will affect release or redaction of BWC recordings from TFO BWCs made while working under federal authority on behalf of ATF ("TFO BWC recordings").
- C. Valencia County Sheriff's Office will notify and consult ATF prior to making any change in agency policy that will affect the storage, release, or redaction of TFO BWC recordings.
- D. Valencia County Sheriff's Office will provide training to ATF task force personnel on the BWCs to familiarize them with the capabilities and operation of BWCs used during task force activities.
- E. Valencia County Sheriff's Office will allow ATF Task Force supervisors to make decisions about recording or not recording under the same circumstances that parent agency supervisors are allowed to make such decisions. Valencia County Sheriff's Office will provide training to ATF personnel as needed to implement this.

V. Handling of BWC Recordings Made During Task Force Operations:

- A. For purposes of this agreement, the term "TFO BWC recordings" refers to audio and video recordings, and associated metadata, from TFO BWCs made while the TFO is working under federal authority.
- B. In accordance with current agency policy and practice, Valencia County Sheriff's Office will provide full, un-redacted copies of TFO BWC recordings to ATF within 72 hours unless approved in writing by the ATF SAC.
- C. TFOs will document BWC use and the existence of BWC recordings in the Report of Investigation (ROI). The TFO will include in the ATF ROI a statement attesting that the date provided is a fair and accurate copy of the data recorded by the BWC.
- D. All TFO BWC recordings made during federal task force operations, including such recordings retained by the Valencia County Sheriff's Office and/or in the possession of any third party engaged by Valencia County Sheriff's Office to store or process BWC recordings shall be deemed federal records of the United States Department of Justice, Bureau of Alcohol, Tobacco, Firearms and Explosives (DOJ/ ATF) pursuant to the Federal Records Act.

Addendum to Task Force Agreements Pertaining to Body Worn Cameras

E. All TFO BWC recordings made during ATF operations in accordance with this agreement, including recordings retained by the TFO Parent Agency and/or in the possession of any third party engaged by the TFO Parent Agency to store or process BWC recordings are federal records of ATF pursuant to the Federal Records Act and may not be disseminated by the TFO or any third party, as described here, without the written permission of ATF.

F. **Internal Dissemination:**

The TFO's parent agency is authorized to use TFO BWC recordings for internal investigations of its personnel consistent with the parent agency's policies and procedures, not involving dissemination outside the parent agency or public release. The parent agency shall provide written notification to the sponsoring federal agency prior to any internal review.

G. **Expedited Public Release:**

If TFO BWC recording(s) depict conduct committed solely by a TFO resulting in serious bodily injury or death of another, the TFO's parent agency shall notify the sponsoring federal agency¹ and the United States Attorney if it intends to publicly release the TFO's BWC recording(s). The sponsoring federal agency and the United States Attorney will expeditiously review the recording(s) and provide official concurrence with public release as soon as practical, unless there are specific and compelling circumstances justifying an objection to public release that cannot be resolved by redaction or other means. Upon official concurrence, the TFO's parent agency may immediately release the recording(s) with any agreed-upon redactions, giving as much advance notice as possible to the sponsoring federal agency and United States Attorney as to the time and manner of its release.

H. In all circumstances, TFO BWC recordings shall be treated as law enforcement sensitive information, the premature disclosure of which could reasonably be expected to interfere with enforcement proceedings, and as potential evidence in a federal investigation subject to applicable federal laws, rules, and policy concerning disclosure or dissemination (including but not limited to 28 C.F.R. Ch. 1, Pt. 16, Subpart B

¹ The notification may be to the Special Agent in Charge (SAC) or the Director of the ATF (or the Director's designee), and any discussions, negotiations, and concurrence may be made by the SAC or Director of ATF (or the Director's designee) after appropriate consultation within their agency.

Addendum to Task Force Agreements Pertaining to Body Worn Cameras

(“Touhy”, absent appropriate redaction prior to disclosure or dissemination).

- I. If a TFO BWC recording involves a use of force incident as defined below, or involves another time-sensitive or urgent situation, Valencia County Sheriff's Office will provide ATF copies on an expedited basis, including during non-business hours. For purposes of this provision, use of force incidents include, but are not limited to, incidents utilizing intermediate weapons, i.e., TASERs, expandable batons, kinetic energy projectiles, emergency/improvised intermediate impact weapons, such as, a flashlight or radio; any use of force resulting in serious injury or death; canine bites resulting in penetration of human skin; and all shooting incidents.
- J. Valencia County Sheriff's Office will provide witnesses as needed to authenticate TFO recordings in ATF cases.
- K. Valencia County Sheriff's Office will inform ATF of the length of time TFO BWC recordings will be retained by the agency before deletion. Valencia County Sheriff's Office will honor any request by ATF to retain the TFO BWC recordings for a longer period of time.
- L. Valencia County Sheriff's Office will restrict access to TFO BWC recordings within the agency as follows: System Administrators, and the evidence custodian.
- M. Valencia County Sheriff's Office will notify ATF immediately of any unauthorized access to TFO recordings discovered by the agency.
- N. Valencia County Sheriff's Office will cooperate fully with ATF in the investigation of any unauthorized access to or disclosure of TFO recordings, including providing ATF the name(s) of any agency personnel determined by the agency to be involved in unauthorized access, copying, or disclosure.
- O. Valencia County Sheriff's Office will notify ATF as soon as possible regarding any request or demand for release or disclosure of TFO recordings, including but not limited to subpoenas, discovery demands or motions, open record/freedom of information requests, media requests, or union or other professional association requests.
- P. Valencia County Sheriff's Office will not publicly release TFO BWC Recordings without the express, written permission of ATF. Further, upon request of ATF, Valencia County Sheriff's Office will withhold public release of any TFO recording.
- Q. Valencia County Sheriff's Office will not release or disseminate TFO recordings to any other law enforcement agency, or to any state or local prosecutor, without the express written permission of ATF.

Addendum to Task Force Agreements Pertaining to Body Worn Cameras

- R. Valencia County Sheriff's Office will redact any video or audio portion of TFO recordings as requested by ATF prior to public release unless doing so would violate a Federal court order. Upon request of ATF, [Name of Police Agency] will permit ATF to redact any TFO recording that will be publicly released.
- S. Valencia County Sheriff's Office will disable any GPS and/or live stream capability with TFO BWCs, and issue agency policy prohibiting TFOs from using GPS or live stream capabilities while working as deputized TFOs under Federal authority.

Signature of Special Agent in Charge Date

(b) (6), (b) (7)(C)

6/22/2021

Signature of Department Official

Date

ATTACHMENT 1

Standard Operating Procedures for Task Force Officer Body-Worn Camera Program

BODY-WORN CAMERA TASK FORCE OFFICER AGENCY CHECKLIST

Complete separate checklist for each agency employing task force officers that will use body-worn cameras (BWC). Attach additional sheets if necessary.

Date: June 22, 2021

ATF Division	Task Force	State/Local Agency
	Albuquerque Group I	Valencia County Sheriff's Office
Person Completing Checklist		
Name	Phone Number	Email Address
(b) (6), (b) (7)(C)	(b) (6), (b) (7)(C)	(b) (6), (b) (7)(C)@co.valencia.nm.us

A. State & Local Legal Authority		
List and attach any state or local laws applicable to BWCs or impacting BWCs (e.g., open records laws, legal retention requirements, etc.); and other pertinent legal guidance (e.g., significant case law, State AG Opinions, etc.). If none, enter "N/A." Add additional rows as necessary.		
Title	Cite	Comments
THE INSPECTION OF PUBLIC RECORDS ACT	NMSA 1978, Chapter 14, Article 2	https://law.justia.com/codes/new-mexico/2011/chapter14/article2/section14-2-1/
Body Cameras while on duty	NMSA 1978, 29-1-18	https://codes.findlaw.com/nm/chapter-29-law-enforcement/nm-st-sect-29-1-18.html
B. TFO Parent Agency Policies		
List and attach any policy, procedure, or other written directive from the TFO's parent agency applicable to TFOs' use of BWCs. Include any union or other labor agreement requirements regarding BWCs applicable to TFOs. If none, enter "N/A." Add additional rows as necessary.		
Title	Cite	Comments
VCSO SOP	VCSO 2-36.01	https://public.powerdms.com/ValenciaCSO/tree

Answer the following questions, including any applicable citation (e.g., state or local law, agency policy, vendor contract, etc.).		
<i>C. BWC System</i>		
1	Name/model of BWC used by agency? Attach technical specifications.	Visual Labs application used on an android smart phone
2	Internal storage of recordings or external with a 3 rd party vendor? If a 3 rd party, identify the vendor, attach contract.	external storage by Visual Labs
3	Does the BWC system include a “buffer” or “pre-record” function, or a “post-record” function? If so, state the length of the buffer/pre-record and/or post-record, and whether it is audio only or both audio and video.	Its does include but it is not active with any of our cameras.
4	Can the system be configured to give designated ATF personnel direct access to view and copy TFO recordings at the ATF office?	Yes a log in can be created for someone at ATF.
5	Will ATF need specialized software or equipment to view recordings? If so, specify.	Internet access or windows media player for downloads
6	Will ATF need specialized software or equipment to copy recordings? If so, specify.	No
7	Does the system have an audit function that will identify persons who accessed, downloaded, or copied recordings?	Yes
8	How will ATF cases be identified in the agency’s system?	The person making the recording can mark it any way they choice
9	What metadata can be obtained from BWC recordings?	Deputy who took the recording, date & time, GPS, speed, tags, bookmarks, and captions
10	How long will recordings be preserved in the agency’s system? Attach any agency retention schedule, and note whether it is mandated by state /local law or agency policy only.	It is decided by the operator making the recording. 6 months minimum to indefinitely.
11	Does the BWC system allow restriction of BWC recording access to specific persons within the agency?	Three levels, Admin, supervisor, and user
12	How does agency handle inadvertent/accidental recordings?	no different than any other recording
13	How does agency handle requests to delete BWC recordings?	we can not delete. recordings are deleted automatically based on retention set by user
14	Will the TFO be able to charge the BWC and/or download/upload the recordings into the agency’s BWC system at the ATF task force office?	recordings are done on a cell phone and are automatically uploaded as long as there is cell service.
15	Does the BWC have a GPS function? If so, is the function available to the TFO, and what is the agency’s policy regarding use of GPS? Can it be deactivated on TFO BWCs?	yes it has GPS and it can not be deactivated.

16	Does the BWC have a “live stream” capability? If so, is the function available to the TFO, and what is the agency’s policy regarding use of “live streaming” with BWCs? Can it deactivated on TFO BWCs?	It does have the capability and cannot be deactivated. can only by done by Lt or above.
17	Does the agency utilize facial recognition technology with BWC recordings?	No.
18	Provide an agency point-of-contact who can provide information regarding system security and protections, and location and security precautions of data storage facilities. *Do not attach this information.*	(b) (6), (b) (7)(C)

<i>D. BWC Use</i>		
1	Are there any exceptions under agency policy to the requirement to record search warrant executions or arrests?	No.
2	What is the agency's policy regarding BWC recording of CSs?	to not record
3	Does agency prohibit BWC recording in any specific situations? If so, list.	undercover operations
4	Under agency policy, are there circumstances when a supervisor may direct the officer to record or not record?	no only to stop recording depending on situation.
5	What is the agency's policy regarding citizen notification of BWC recording?	no requirement to notify citizens
6	If the TFO's BWC is inoperable does the agency's policy permit the TFO to participate in enforcement activities if a replacement is not readily available?	yes but the incident must be documented.

E. Law Enforcement Access to BWC Recordings		
1	Are officers allowed to review BWC recordings before writing reports? Giving statements? <ul style="list-style-type: none"> If so, are they allowed to view only recordings from their own BWC, or are they allowed view BWC recordings from other officers? 	Yes they can review their recordings. Only supervisors can review others recordings. they can review but someone else must show them the recording.
2	If officers are allowed to review recordings are there any exceptions? If so list the exceptions, e.g., internal investigations, critical incidents (e.g., officer-involved shooting (OIS), use of deadly force, etc.)?	With an OIS they don't review until they have meet with their attorney.
3	Who in the parent agency will have access to TFOs' BWC recordings involving ATF/federal cases?	Admins, supervisors and evidence custodian.
4	Does agency restrict access to BWC recordings involving a critical incident (e.g., OIS)? If so, who has access in those situations?	no we do not restrict access unless there is a specific need.
5	Will members of the parent agency be able to identify ATF cases in the BWC system? How?	The TFO can "tag" the recording with relevant info
6	Does the agency require random or directed supervisory review/audit of officer videos for policy compliance or other issues? If so, will this include TFO recordings of ATF cases?	no requirement to audit recordings.
7	Will non-law enforcement employees of the parent agency or municipality have access to ATF BWC recordings, e.g., IT? If so, are they CJIS-compliant (e.g., CJIS background checks)?	The only no LE person with access are the two evidence custodians and IT person all have had a CJIS background checks.
8	Are officers allowed to make copies of BWC recordings, or must they obtain recordings from someone else within the agency?	They can download recordings.
9	Are officers allowed to possess copies of recordings outside the police facility, or retain possession of copies for personal use?	Not unless they submit a request just as any other citizen could.
10	Does the agency have a policy prohibiting sharing of recordings outside of law enforcement for non-official reasons?	Yes we do.
11	Does the agency have a policy prohibiting the posting of BWC recordings to the Internet, social media sites, or the media for non-official purposes?	yes we do.
12	Does the agency have a policy prohibiting officers from wearing or using privately owned BWCs or any other non-issued BWC?	yes we do.
13	Do any other law enforcement entities or personnel have direct access to recordings, e.g., prosecutor's office?	not at this time.

14	<p>Does the parent agency investigate TFO-involved shootings (or other TFO-involved events involving death or serious injury), or is this done by another agency? If another agency:</p> <ul style="list-style-type: none"> • Identify the agency. • Is there an agreement, policy, or protocol in place with the agency for handling these situations? If so, attach. 	<p>No we do not, NM State Police has done all of our OIS events. There is no written agreement for this.</p>
-----------	--	--

F. External Access to BWC Recordings		
1	<p>How does the agency handle external requests for BWC recordings?</p> <ul style="list-style-type: none"> • Criminal discovery, subpoenas? • Civil/administrative discovery, subpoenas? • Open record/freedom of information requests? • Media requests? • Union requests? Is there an agreement with the union regarding union disclosure of BWC recordings? If so, attach copy. 	<p>locate recording, asses if they have to pay, redact if required, and then sent recording.</p> <p>There is no union agreement for the recordings.</p>
2	<p>If the agency uses a 3rd party vendor to store recordings:</p> <ul style="list-style-type: none"> • is security of or access to recordings addressed in the contract? • are background checks of vendor employees addressed in the contract? <p>If so, attach copy.</p>	<p>Yes data stored on Microsoft Azure Government Cloud</p>
3	<p>How does the agency handle redaction of BWC recordings prior to public release?</p>	<p>yes we do.</p>

To: (b) (6), (b) (7)(C)
From: (b) (6), (b) (7)(C)
Sent: Thur 7/1/2021 8:03:41 PM
Subject: RE: New Mexico TFO MOU
MOU Valencia County June 2021 SIGNED.pdf
TFO BWC Addendum Valencia Co signed.pdf
ATF BWC-TFO Checklist Valencia County June 2021.pdf

(b) (6), (b) (7)(C) attached are the TFO MOU, BWC Addendum, and BWC Checklist from Valencia County Sheriff's Office. Thank you.

From: (b) (6), (b) (7)(C)
Sent: Wednesday, June 30, 2021 4:29 AM
To: (b) (6), (b) (7)(C)
Subject: RE: New Mexico TFO MOU

(b) (6), (b) (7)(C)

I reviewed the documents. Once the SAC has signed the addendum, please send me the completed documents and we will get your group scheduled for Evidence.com training. Thanks!

(b) (6), (b) (7)(C)
Alcohol, Tobacco, Firearms and Explosives
16009 N. 81st Street, Suite 100
Scottsdale, AZ 85260
Special Agent Project Officer-Digital Evidence Management
Technical Project Office
Special Operations Division
(b) (6), (b) (7)(C)

CONFIDENTIALITY NOTICE: E-mail may contain confidential information that is legally privileged. Do not read this e-mail if you are not the intended recipient.

This e-mail transmission, and any documents, files or previous e-mail messages attached to it may contain confidential information that is legally privileged. If you are not the intended recipient, or a person responsible for delivering it to the intended recipient, you are hereby notified that any disclosure, copying, distribution or use of any of the information contained in or attached to this transmission is STRICTLY PROHIBITED. If you have received this transmission in error, please immediately notify us by reply e-mail, by forwarding this to (b) (6), (b) (7)(C) or by telephone at (b) (6), (b) (7)(C) and destroy the original transmission and its attachments without reading or saving in any manner. Thank you.

From: (b) (6), (b) (7)(C)
Sent: Tuesday, June 29, 2021 12:30 PM
To: (b) (6), (b) (7)(C)
Subject: New Mexico TFO MOU

Hello (b) (6), (b) (7)(C) the one sheriff's office that you were on standby for a few weeks ago has returned the BWC docs. Could you take a look at them please? A couple things I noticed on the Addendum:

(b) (5)

(b) (5)

Thank you,

(b) (6), (b) (7)(C)

MEMORANDUM OF UNDERSTANDING

BETWEEN

THE BUREAU OF ALCOHOL, TOBACCO, FIREARMS AND EXPLOSIVES (“ATF”)

AND

THE VALENCIA COUNTY SHERIFF’S OFFICE (“VCSO”)

This Memorandum of Understanding (“MOU”) is entered into by and between the Bureau of Alcohol, Tobacco, Firearms and Explosives (“ATF”) and the Valencia County Sheriff’s Office (“VCSO” and “participating agency”) as it relates to the ATF Albuquerque Group I Task Force (herein referred to as the “Task Force”).

AUTHORITIES

The authority to investigate and enforce offenses under provisions of this MOU are found at 28 U.S.C. § 599A, 28 C.F.R. §§ 0.130, 0.131, and 18 U.S.C. § 3051.

PURPOSE

The Task Force will perform the activities and duties described below:

- a. Investigate firearms-related violent crime and other crimes of violence
- b. Investigate firearms trafficking and straw purchasing
- c. Investigate unlawful firearms possession
- d. Investigate armed narcotics trafficking
- e. Investigate violent criminal gangs and organizations
- f. Investigate arsons and explosives violations
- g. Conduct complex criminal investigations utilizing all appropriate investigative techniques so that the Task Force's activities will result in effective and impactful prosecutions in the courts of the United States and/or the State of New Mexico

MEASUREMENT OF SUCCESS

The success of this initiative will be measured by performance indicators such as the number of violent offenders referred for prosecution; percentage of all firearms cases referred for prosecution ultimately indicted and/or convicted; the number of criminal conspiracies or organizations referred for prosecution; the number of crime guns recovered; the number of proactive criminal investigations opened; the number and diversity of investigative techniques and tools utilized.

PHYSICAL LOCATION

Officers/troopers/agents assigned to this Task Force by their employer shall be referred to as Task Force Officers (TFOs). TFOs will be assigned to the ATF Albuquerque Group I Field Office and will be located at 201 Third Street NW, Suite 1550, Albuquerque, New Mexico, and will also utilize the Valencia County Sheriff's Office, Los Lunas, New Mexico, to fulfill the investigative mission of the Task Force.

SUPERVISION AND CONTROL

The day-to-day supervision and administrative control of TFOs will be the mutual responsibility of the participants, with the ATF Resident Agent in Charge or his/her designee having operational control over all operations related to this Task Force.

Each TFO shall remain subject to their respective agencies' policies, and shall report to their respective agencies regarding matters unrelated to this agreement/task force. With regard to matters related to the Task Force, TFOs will be subject to Federal law and Department of Justice (DOJ) and ATF orders, regulations and policy, including those related to standards of conduct, sexual harassment, equal opportunity issues and Federal disclosure laws.

Failure to comply with this paragraph could result in a TFO's dismissal from the Task Force.

PERSONNEL, RESOURCES AND SUPERVISION

To accomplish the objectives of the Task Force, ATF will assign eight (8) Special Agents to the Task Force. ATF will also, subject to the availability of funds, provide necessary funds and equipment to support the activities of the ATF Special Agents and officers assigned to the Task Force. This support may include: office space, office supplies, travel funds, funds for the purchase of evidence and information, investigative equipment, training, and other support items.

Each participating agency agrees to make available to their assigned Task Force members any equipment ordinarily assigned for use by that agency. In the event ATF supplies equipment (which may include vehicles, weapons or radios), TFOs must abide by any applicable ATF property orders or policy, and may be required to enter into a separate agreement for their use.

To accomplish the objectives of the Task Force, the Valencia County Sheriff's Office agrees to detail one (1) part-time TFO to the Task Force for a period of not less than two (2) years.

All TFOs shall qualify with their respective firearms by complying with ATF's Firearms and Weapons Policy.

SECURITY CLEARANCES

All TFOs will undergo a security clearance and background investigation, and ATF shall bear the costs associated with those investigations. TFOs must not be the subject of any ongoing

investigation by their department or any other law enforcement agency, and past behavior or punishment, disciplinary, punitive or otherwise, may disqualify one from eligibility to join the Task Force. ATF has final authority as to the suitability of TFOs for inclusion on the Task Force.

DEPUTATIONS

ATF, as the sponsoring Federal law enforcement agency, may request at its sole discretion that the participating agency's TFOs be deputized by the U.S. Marshals Service to extend their jurisdiction, to include applying for and executing Federal search and arrest warrants, and requesting and executing Federal grand jury subpoenas for records and evidence involving violations of Federal laws. Such requests will be made on an individual basis as determined by ATF.

A TFO will not be granted Department of Justice legal representation if named as a defendant in a private-capacity lawsuit alleging constitutional violations unless all deputation paperwork has been completed prior to the event(s) at issue in the lawsuit.

The participating agencies agree that any Federal authority that may be conferred by a deputation is limited to activities supervised by ATF and will terminate when this MOU is terminated or when the deputized TFOs leave the Task Force, or at the discretion of ATF.

ASSIGNMENTS, REPORTS AND INFORMATION SHARING

An ATF supervisor or designee will be empowered with designated oversight for investigative and personnel matters related to the Task Force and will be responsible for opening, monitoring, directing and closing Task Force investigations in accordance with ATF policy and the applicable United States Attorney General's Guidelines.

Assignments will be based on, but not limited to, experience, training, and performance, in addition to the discretion of the ATF supervisor.

All investigative reports will be prepared utilizing ATF's investigative case management system, (N-Force) utilizing ATF case report numbers. The participating agency will share investigative reports, findings, intelligence, etc., in furtherance of the mission of this agreement, to the fullest extent allowed by law. For the purposes of uniformity, there will be no duplication of reports, but rather a single report prepared by a designated individual which can be duplicated as necessary. Every effort should be made to document investigative activity on ATF Reports of Investigation (ROI), unless otherwise agreed to by ATF and the participating agency(ies). This section does not preclude the necessity of individual TFOs to complete forms required by their employing agency.

Information will be freely shared among the TFOs and ATF personnel with the understanding that all investigative information will be kept strictly confidential and will only be used in furtherance of criminal investigations. No information gathered during the course of the Task Force, to include informal communications between TFOs and ATF personnel, may be

disseminated to any third party, non-task force member by any task force member without the express permission of the ATF Special Agent in Charge or his/her designee.

Any public requests for access to the records or any disclosures of information obtained by task force members during Task Force investigations will be handled in accordance with applicable statutes, regulations, and policies pursuant to the Freedom of Information Act and the Privacy Act and other applicable federal and/or state statutes and regulations.

INVESTIGATIVE METHODS

The parties agree to utilize Federal standards pertaining to evidence handling and electronic surveillance activities to the greatest extent possible. However, in situations where state or local laws are more restrictive than comparable Federal law, investigative methods employed by state and local law enforcement agencies shall conform to those requirements, pending a decision as to a venue for prosecution.

The use of other investigative methods (search warrants, interceptions of oral communications, etc.) and reporting procedures in connection therewith will be consistent with the policy and procedures of ATF. All Task Force operations will be conducted and reviewed in accordance with applicable ATF and Department of Justice policy and guidelines.

None of the parties to this MOU will knowingly seek investigations under this MOU that would cause a conflict with any ongoing investigation of an agency not party to this MOU. It is incumbent upon each participating agency to notify its personnel regarding the Task Force's areas of concern and jurisdiction. All law enforcement actions will be coordinated and cooperatively carried out by all parties to this MOU.

INFORMANTS

ATF guidelines and policy regarding the operation of informants and cooperating witnesses will apply to all informants and cooperating witnesses directed by TFOs.

Informants developed by TFOs may be registered as informants of their respective agencies for administrative purposes and handling. The policies and procedures of the participating agency with regard to handling informants will apply to all informants that the participating agency registers. In addition, it will be incumbent upon the registering participating agency to maintain a file with respect to the performance of all informants or witnesses it registers. All information obtained from an informant and relevant to matters within the jurisdiction of this MOU will be shared with all parties to this MOU. The registering agency will pay all reasonable and necessary informant expenses for each informant that a participating agency registers.

DECONFLICTION

Each participating agency agrees that the deconfliction process requires the sharing of certain operational information with the Task Force, which, if disclosed to unauthorized persons, could

endanger law enforcement personnel and the public. As a result of this concern, each participating agency agrees to adopt security measures set forth herein:

- a. Each participating agency will assign primary and secondary points of contact.
- b. Each participating agency agrees to keep its points of contact list updated.

The points of contact for this Task Force are:

ATF: (Primary) Resident Agent in Charge Patrick Henning, Albuquerque Group I Field Office
(Secondary) Senior Special Agent Kevin Wolfe, Albuquerque Group I Field Office

Participating Agency: (Primary) Deputy Rashad Pearson, Valencia County Sheriff's Office
(Secondary) Undersheriff Jeff Noah, Valencia County Sheriff's Office

EVIDENCE

Evidence will be maintained by the lead agency having jurisdiction in the court system intended for prosecution. Evidence generated from investigations initiated by a TFO or ATF special agent intended for Federal prosecution will be placed in the ATF designated vault, using the procedures found in ATF orders.

All firearms seized by a TFO must be submitted for fingerprint analysis and for a National Integrated Ballistic Information Network (NIBIN) examination. Once all analyses are completed, all firearms seized under Federal law shall be placed into the ATF designated vault for proper storage. All firearms information/descriptions taken into ATF custody must be submitted to ATF's National Tracing Center.

JURISDICTION/PROSECUTIONS

Cases will be reviewed by the ATF Special Agent in Charge or his/her designee in consultation with the participating agency and the United States Attorney's Office and appropriate State's attorney offices, to determine whether cases will be referred for prosecution to the U.S. Attorney's Office or to the relevant State's attorney's office. This determination will be based upon which level of prosecution will best serve the interests of justice and the greatest overall benefit to the public. Any question that arises pertaining to prosecution will be resolved through discussion among the investigative agencies and prosecuting entities having an interest in the matter.

In the event that a state or local matter is developed that is outside the jurisdiction of ATF or it is decided that a case will be prosecuted on the state or local level, ATF will provide all relevant information to state and local authorities, subject to Federal law. Whether to continue investigation of state and local crimes is at the sole discretion of the state or local participating agency.

USE OF FORCE

All TFOs will comply with ATF and the Department of Justice's (DOJ's) Use of Force orders and policies. TFOs must be briefed on ATF's and DOJ's Use of Force policy by an ATF official, and will be provided with a copy of such policy.

BODY WORN CAMERAS AND TASK FORCE OFFICERS

In accordance with DOJ policy, dated October 29, 2020, Body Worn Cameras (BWCs) may be worn by TFOs operating on a Federal Task Force when their parent agency mandates their use by personnel assigned to the task force. In such cases, the parent agency must formally request to participate in the TFO BWC program and, upon approval, shall comply with all DOJ and ATF policies, and the required procedures, documentation, and reporting while participating on the task force.

MEDIA

Media relations will be handled by ATF and the U.S. Attorney's Office's public information officers in coordination with each participating agency. Information for press releases will be reviewed and mutually agreed upon by all participating agencies, who will take part in press conferences. Assigned personnel will be informed not to give statements to the media concerning any ongoing investigation or prosecution under this MOU without the concurrence of the other participants and, when appropriate, the relevant prosecutor's office.

All personnel from the participating agencies shall strictly adhere to the requirements of Title 26, United States Code, § 6103. Disclosure of tax return information and tax information acquired during the course of investigations involving National Firearms Act (NFA) firearms as defined in 26 U.S.C., Chapter 53 shall not be made except as provided by law.

SALARY/OVERTIME COMPENSATION

During the period of the MOU, participating agencies will provide for the salary and employment benefits of their respective employees. All participating agencies will retain control over their employees' work hours, including the approval of overtime.

ATF may have funds available to reimburse overtime to the State and Local TFO's agency, subject to the guidelines of the Department of Justice Asset Forfeiture Fund. This funding would be available under the terms of a memorandum of agreement (MOA) established pursuant to the provisions of 28 U.S.C. section 524. The participating agency agrees to abide by the applicable Federal law and policy with regard to the payment of overtime from the Department of Justice Asset Forfeiture Fund. The participating agency must be recognized under State law as a law enforcement agency and their officers/ troopers/investigators as sworn law enforcement officers. If required or requested, the participating agency shall be responsible for demonstrating to the Department of Justice that its personnel are law enforcement officers for the purpose of overtime payment from the Department of Justice Asset Forfeiture Fund. **This MOU is not a funding document.**

In accordance with these provisions and any MOA on asset forfeiture, the ATF Special Agent in Charge or designee shall be responsible for certifying reimbursement requests for overtime expenses incurred as a result of this agreement.

AUDIT INFORMATION

Operations under this MOU are subject to audit by ATF, the Department of Justice's Office of the Inspector General, the Government Accountability Office, and other Government-designated auditors. Participating agencies agree to permit such audits and to maintain all records relating to Department of Justice Asset Forfeiture Fund payments for expenses either incurred during the course of this Task Force or for a period of not less than three (3) years and, if an audit is being conducted, until such time that the audit is officially completed, whichever is greater.

FORFEITURES/SEIZURES

All assets seized for administrative forfeiture will be seized and forfeited in compliance with the rules and regulations set forth by the U.S. Department of Justice Asset Forfeiture guidelines. When the size or composition of the item(s) seized make it impossible for ATF to store it, any of the participating agencies having the storage facilities to handle the seized property agree to store the property at no charge and to maintain the property in the same condition as when it was first taken into custody. The agency storing said seized property agrees not to dispose of the property until authorized to do so by ATF.

The MOU provides that proceeds from forfeitures will be shared, with sharing percentages based upon the U.S. Department of Justice Asset Forfeiture policies on equitable sharing of assets, such as determining the level of involvement by each participating agency. Task Force assets seized through administrative forfeiture will be distributed in equitable amounts based upon the number of full-time persons committed by each participating agency. Should it become impossible to separate the assets into equal shares, it will be the responsibility of all the participating agencies to come to an equitable decision. If this process fails and an impasse results, ATF will become the final arbitrator of the distributive shares for the participating agencies

DISPUTE RESOLUTION

In cases of overlapping jurisdiction, the participating agencies agree to work in concert to achieve the Task Force's goals and objectives. The parties to this MOU agree to attempt to resolve any disputes regarding jurisdiction, case assignments and workload at the lowest level possible.

LIABILITY

ATF acknowledges that the United States is liable for the wrongful or negligent acts or omissions of its officers and employees, including TFOs, while on duty and acting within the scope of their federal employment, to the extent permitted by the Federal Tort Claims Act.

Claims against the United States for injury or loss of property, personal injury, or death arising or resulting from the negligent or wrongful act or omission of any Federal employee while acting within the scope of his or her office or employment are governed by the Federal Tort Claims Act, 28 U.S.C. sections 1346(b), 2672-2680 (unless the claim arises from a violation of the Constitution of the United States, or a violation of a statute of the United States under which other recovery is authorized).

Except as otherwise provided, the parties agree to be solely responsible for the negligent or wrongful acts or omissions of their respective employees and will not seek financial contributions from the other for such acts or omissions. Legal representation by the United States is determined by the United States Department of Justice on a case-by-case basis. ATF cannot guarantee the United States will provide legal representation to any State or local law enforcement officer.

Liability for any negligent or willful acts of any agent or officer undertaken outside the terms of this MOU will be the sole responsibility of the respective agent or officer and agency involved.

DURATION

This MOU is effective with the signatures of all parties and terminates at the close of business on September 30, 2026.

This MOU supersedes previously signed MOUs and shall remain in effect until the aforementioned expiration date or until it is terminated in writing (to include electronic mail and facsimile), whichever comes first. All participating agencies agree that no agency shall withdraw from the Task Force without providing ninety (90) days written notice to other participating agencies. If any participating agency withdraws from the Task Force prior to its termination, the remaining participating agencies shall determine the distributive share of assets for the withdrawing agency, in accordance with Department of Justice guidelines and directives.

The MOU shall be deemed terminated at the time all participating agencies withdraw and ATF elects not to replace such members, or in the event ATF unilaterally terminates the MOU upon 90 days written notice to all the remaining participating agencies.

MODIFICATIONS

This agreement may be modified at any time by written consent of all participating agencies. Modifications shall have no force and effect unless such modifications are reduced to writing and signed by an authorized representative of each participating agency.

SIGNATURES

(b) (6), (b) (7)(C)

Denise Vigil
Sheriff
Valencia County Sheriff's Office

6/22/2021

Date

(b) (6), (b) (7)(C)

Gabriel R. Pinon
Special Agent in Charge, ATF
Phoenix Field Division

6/24/21

Date

(b) (6), (b) (7)(C)

Undersheriff

Valencia County Sheriff's Office

6.22.21

Date

Addendum to Task Force Agreements Pertaining to Body Worn Cameras

This addendum supplements the agreement between the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and the Valencia County Sheriff's Office dated June 22, 2021, establishing the Albuquerque Group I Task Force Pursuant to the "Department of Justice Policy – Use of Body-Worn Cameras (BWC) by Federally Deputized Task Force Officers," dated June 10/28/2021. Valencia County Sheriff's Office has advised ATF that it will require its deputized officers participating in the Task Force to use Body Worn Cameras (BWCs). This addendum governs that use.

10/28/2021
6:00 PM

The parties hereby agree to the following:

- I. TFOs will adhere to the DOJ Policy, ATF's Standard Operating Procedures for Task Force Officer Body Camera Program, and other applicable ATF policies and procedures.
- II. Valencia County Sheriff's Office confirms that prior to executing this agreement it has provided to ATF details regarding the BWC system and cameras, including the details of any system protections, and any state or local policies or laws applicable to the TFO's use of BWCs, including any retention policies as detailed in Attachment I – Agency Checklist.
- III. Use of BWCs During Federal Task Force Operations:
 - A. Deputized Task Force Officers (TFO) through the Joint Law Enforcement Operations (JLEO) Program will be allowed to wear and activate their recording equipment with BWCs for the purposes of recording their actions only during:
 1. A planned attempt to serve an arrest warrant or other planned arrest; or
 2. The execution of a search warrant.
 - B. TFOs are authorized to activate their BWCs upon making entry into a premises or upon approaching a subject, and must deactivate their BWCs when the scene is secured as determined by the federal supervisor on the scene as designated by the sponsoring federal agency.
 1. For purposes of this agreement, the term "secured" means that the scene is safe and under law enforcement control.
 2. In the event circumstances arise requiring additional law enforcement assistance to secure the scene, the TFO will end BWC recording when relieved from the scene by another law enforcement agency.
 3. For the execution of a search warrant, BWCs should not be used for searches of property lawfully in government custody or control, or a search to obtain digital or electronic records executed by a third party, such as an electronic service provider or custodian of electronic records.

Addendum to Task Force Agreements Pertaining to Body Worn Cameras

- C. TFOs will follow the provisions set forth in this agreement for use of BWCs, and the provisions of this agreement will supersede any conflicting provision in the agency's policy for TFOs while serving on the federal Task Force.**
- D. TFOs may use BWCs in accordance with this policy anywhere they are authorized to act as a police or peace officer under state, local, territorial or tribal law.**
- E. TFOs may use only agency-issued and agency-owned BWCs. TFOs will not be allowed to possess or use any privately owned BWC or other recording device of any kind.**
- F. In the event a TFO's BWC is not working or inoperable due to a technical problem or cannot be used due to physical damage, and, in the judgement of the Task Force supervisor, delaying the operation to repair or obtain a replacement BWC is not practical or would impair the operation, the TFO may participate in the operation without using a BWC.**
- G. Even when BWC use would be permissible in the circumstances set forth in Section III A above, TFOs are prohibited from recording;**
 - 1. Undercover personnel;**
 - 2. Confidential informants or confidential sources;**
 - 3. On-scene witness interviews prior to or after the operation;**
 - 4. Personnel using specialized investigative techniques or equipment; or**
 - 5. Actions by any non-law enforcement persons at the scene who are assisting law enforcement personnel.**
- H. Even when BWC use would be permissible in the circumstances set forth above in Section III A above, TFOs are prohibited from activating their BWC if, in the judgement of the ATF, the TFO:**
 - 1. National Security (including international and domestic terrorism investigations or cases involving classified information);**
 - 2. Public Corruption;**
 - 3. Medical Facilities; or**
 - 4. Other sensitive investigations as determined by ATF.**
- I. Even when BWC use would be permissible in the circumstances set forth in Section III A above, TFOs shall not use BWCs to record any activities related to:**
 - 1. Is using specialized or sensitive investigative techniques;**
 - 2. Is operating in a sensitive area; or**
 - 3. Is working in an undercover or covert status on behalf of the federal task force.**

Addendum to Task Force Agreements Pertaining to Body Worn Cameras

IV. Valencia County Sheriff's Office Internal Controls:

- A. Undersheriff Jeff Noah will serve as a point-of-contact (POC) for ATF on BWC matters.**
- B. Valencia County Sheriff's Office will notify ATF of any change in state or local law that will modify how ATF TFOs must use BWCs or will affect release or redaction of BWC recordings from TFO BWCs made while working under federal authority on behalf of ATF ("TFO BWC recordings").**
- C. Valencia County Sheriff's Office will notify and consult ATF prior to making any change in agency policy that will affect the storage, release, or redaction of TFO BWC recordings.**
- D. Valencia County Sheriff's Office will provide training to ATF task force personnel on the BWCs to familiarize them with the capabilities and operation of BWCs used during task force activities.**
- E. Valencia County Sheriff's Office will allow ATF Task Force supervisors to make decisions about recording or not recording under the same circumstances that parent agency supervisors are allowed to make such decisions. Valencia County Sheriff's Office will provide training to ATF personnel as needed to implement this.**

V. Handling of BWC Recordings Made During Task Force Operations:

- A. For purposes of this agreement, the term "TFO BWC recordings" refers to audio and video recordings, and associated metadata, from TFO BWCs made while the TFO is working under federal authority.**
- B. In accordance with current agency policy and practice, Valencia County Sheriff's Office will provide full, un-redacted copies of TFO BWC recordings to ATF within 72 hours unless approved in writing by the ATF SAC.**
- C. TFOs will document BWC use and the existence of BWC recordings in the Report of Investigation (ROI). The TFO will include in the ATF ROI a statement attesting that the date provided is a fair and accurate copy of the data recorded by the BWC.**
- D. All TFO BWC recordings made during federal task force operations, including such recordings retained by the Valencia County Sheriff's Office and/or in the possession of any third party engaged by Valencia County Sheriff's Office to store or process BWC recordings shall be deemed federal records of the United States Department of Justice, Bureau of Alcohol, Tobacco, Firearms and Explosives (DOJ/ ATF) pursuant to the Federal Records Act.**

Addendum to Task Force Agreements Pertaining to Body Worn Cameras

- E. All TFO BWC recordings made during ATF operations in accordance with this agreement, including recordings retained by the TFO Parent Agency and/or in the possession of any third party engaged by the TFO Parent Agency to store or process BWC recordings are federal records of ATF pursuant to the Federal Records Act and may not be disseminated by the TFO or any third party, as described here, without the written permission of ATF.**

F. Internal Dissemination:

The TFO's parent agency is authorized to use TFO BWC recordings for internal investigations of its personnel consistent with the parent agency's policies and procedures, not involving dissemination outside the parent agency or public release. The parent agency shall provide written notification to the sponsoring federal agency prior to any internal review.

G. Expedited Public Release:

If TFO BWC recording(s) depict conduct committed solely by a TFO resulting in serious bodily injury or death of another, the TFO's parent agency shall notify the sponsoring federal agency¹ and the United States Attorney if it intends to publicly release the TFO's BWC recording(s). The sponsoring federal agency and the United States Attorney will expeditiously review the recording(s) and provide official concurrence with public release as soon as practical, unless there are specific and compelling circumstances justifying an objection to public release that cannot be resolved by redaction or other means. Upon official concurrence, the TFO's parent agency may immediately release the recording(s) with any agreed-upon redactions, giving as much advance notice as possible to the sponsoring federal agency and United States Attorney as to the time and manner of its release.

- H. In all circumstances, TFO BWC recordings shall be treated as law enforcement sensitive information, the premature disclosure of which could reasonably be expected to interfere with enforcement proceedings, and as potential evidence in a federal investigation subject to applicable federal laws, rules, and policy concerning disclosure or dissemination (including but not limited to 28 C.F.R. Ch. 1, Pt. 16, Subpart B**

¹ The notification may be to the Special Agent in Charge (SAC) or the Director of the ATF (or the Director's designee), and any discussions, negotiations, and concurrence may be made by the SAC or Director of ATF (or the Director's designee) after appropriate consultation within their agency.

Addendum to Task Force Agreements Pertaining to Body Worn Cameras

(“Touhy”, absent appropriate redaction prior to disclosure or dissemination).

- I. If a TFO BWC recording involves a use of force incident as defined below, or involves another time-sensitive or urgent situation, Valencia County Sheriff's Office will provide ATF copies on an expedited basis, including during non-business hours. For purposes of this provision, use of force incidents include, but are not limited to, incidents utilizing intermediate weapons, i.e., TASERs, expandable batons, kinetic energy projectiles, emergency/improvised intermediate impact weapons, such as, a flashlight or radio; any use of force resulting in serious injury or death; canine bites resulting in penetration of human skin; and all shooting incidents.
- J. Valencia County Sheriff's Office will provide witnesses as needed to authenticate TFO recordings in ATF cases.
- K. Valencia County Sheriff's Office will inform ATF of the length of time TFO BWC recordings will be retained by the agency before deletion. Valencia County Sheriff's Office will honor any request by ATF to retain the TFO BWC recordings for a longer period of time.
- L. Valencia County Sheriff's Office will restrict access to TFO BWC recordings within the agency as follows: System Administrators, and the evidence custodian.
- M. Valencia County Sheriff's Office will notify ATF immediately of any unauthorized access to TFO recordings discovered by the agency.
- N. Valencia County Sheriff's Office will cooperate fully with ATF in the investigation of any unauthorized access to or disclosure of TFO recordings, including providing ATF the name(s) of any agency personnel determined by the agency to be involved in unauthorized access, copying, or disclosure.
- O. Valencia County Sheriff's Office will notify ATF as soon as possible regarding any request or demand for release or disclosure of TFO recordings, including but not limited to subpoenas, discovery demands or motions, open record/freedom of information requests, media requests, or union or other professional association requests.
- P. Valencia County Sheriff's Office will not publicly release TFO BWC Recordings without the express, written permission of ATF. Further, upon request of ATF, Valencia County Sheriff's Office will withhold public release of any TFO recording.
- Q. Valencia County Sheriff's Office will not release or disseminate TFO recordings to any other law enforcement agency, or to any state or local prosecutor, without the express written permission of ATF.

Addendum to Task Force Agreements Pertaining to Body Worn Cameras

- R. Valencia County Sheriff's Office will redact any video or audio portion of TFO recordings as requested by ATF prior to public release unless doing so would violate a Federal court order. Upon request of ATF, [Name of Police Agency] will permit ATF to redact any TFO recording that will be publicly released.
- S. Valencia County Sheriff's Office will disable any GPS and/or live stream capability with TFO BWCs, and issue agency policy prohibiting TFOs from using GPS or live stream capabilities while working as deputized TFOs under Federal authority.

(b) (6), (b) (7)(C)

Signature of Special Agent in Charge

Date

7/1/21

(b) (6), (b) (7)(C)

Signature of Department Official

Date

6/22/2021

ATTACHMENT 1

Standard Operating Procedures for Task Force Officer Body-Worn Camera Program

BODY-WORN CAMERA TASK FORCE OFFICER AGENCY CHECKLIST

Complete separate checklist for each agency employing task force officers that will use body-worn cameras (BWC). Attach additional sheets if necessary.

Date: June 22, 2021

ATF Division	Task Force	State/Local Agency
	Albuquerque Group I	Valencia County Sheriff's Office
Person Completing Checklist		
Name	Phone Number	Email Address
(b) (6), (b) (7)(C)	(b) (6), (b) (7)(C)	(b) (6), (b) (7)(C)@co.valencia.nm.us

A. State & Local Legal Authority		
List and attach any state or local laws applicable to BWCs or impacting BWCs (e.g., open records laws, legal retention requirements, etc.); and other pertinent legal guidance (e.g., significant case law, State AG Opinions, etc.). If none, enter "N/A." Add additional rows as necessary.		
Title	Cite	Comments
THE INSPECTION OF PUBLIC RECORDS ACT	NMSA 1978, Chapter 14, Article 2	https://law.justia.com/codes/new-mexico/2011/chapter14/article2/section14-2-1/
Body Cameras while on duty	NMSA 1978, 29-1-18	https://codes.findlaw.com/nm/chapter-29-law-enforcement/nm-st-sect-29-1-18.html
B. TFO Parent Agency Policies		
List and attach any policy, procedure, or other written directive from the TFO's parent agency applicable to TFOs' use of BWCs. Include any union or other labor agreement requirements regarding BWCs applicable to TFOs. If none, enter "N/A." Add additional rows as necessary.		
Title	Cite	Comments
VCSO SOP	VCSO 2-36.01	https://public.powerdms.com/ValenciaCSO/tree

Answer the following questions, including any applicable citation (e.g., state or local law, agency policy, vendor contract, etc.).		
C. BWC System		
1	Name/model of BWC used by agency? Attach technical specifications.	Visual Labs application used on an android smart phone
2	Internal storage of recordings or external with a 3 rd party vendor? If a 3 rd party, identify the vendor, attach contract.	external storage by Visual Labs
3	Does the BWC system include a “buffer” or “pre-record” function, or a “post-record” function? If so, state the length of the buffer/pre-record and/or post-record, and whether it is audio only or both audio and video.	Its does include but it is not active with any of our cameras.
4	Can the system be configured to give designated ATF personnel direct access to view and copy TFO recordings at the ATF office?	Yes a log in can be created for someone at ATF.
5	Will ATF need specialized software or equipment to view recordings? If so, specify.	Internet access or windows media player for downloads
6	Will ATF need specialized software or equipment to copy recordings? If so, specify.	No
7	Does the system have an audit function that will identify persons who accessed, downloaded, or copied recordings?	Yes
8	How will ATF cases be identified in the agency’s system?	The person making the recording can mark it any way they choice
9	What metadata can be obtained from BWC recordings?	Deputy who took the recording, date & time, GPS, speed, tags, bookmarks, and captions
10	How long will recordings be preserved in the agency’s system? Attach any agency retention schedule, and note whether it is mandated by state /local law or agency policy only.	It is decided by the operator making the recording. 6 months minimum to indefinitely.
11	Does the BWC system allow restriction of BWC recording access to specific persons within the agency?	Three levels, Admin, supervisor, and user
12	How does agency handle inadvertent/accidental recordings?	no different than any other recording
13	How does agency handle requests to delete BWC recordings?	we can not delete. recordings are deleted automatically based on retention set by user
14	Will the TFO be able to charge the BWC and/or download/upload the recordings into the agency’s BWC system at the ATF task force office?	recordings are done on a cell phone and are automatically uploaded as long as there is cell service.
15	Does the BWC have a GPS function? If so, is the function available to the TFO, and what is the agency’s policy regarding use of GPS? Can it be deactivated on TFO BWCs?	yes it has GPS and it can not be deactivated.

16	Does the BWC have a “live stream” capability? If so, is the function available to the TFO, and what is the agency’s policy regarding use of “live streaming” with BWCs? Can it deactivated on TFO BWCs?	It does have the capability and cannot be deactivated. can only by done by Lt or above.
17	Does the agency utilize facial recognition technology with BWC recordings?	No.
18	Provide an agency point-of-contact who can provide information regarding system security and protections, and location and security precautions of data storage facilities. <i>*Do not attach this information.*</i>	(b) (6), (b) (7)(C)

<i>D. BWC Use</i>		
1	Are there any exceptions under agency policy to the requirement to record search warrant executions or arrests?	No.
2	What is the agency's policy regarding BWC recording of CSs?	to not record
3	Does agency prohibit BWC recording in any specific situations? If so, list.	undercover operations
4	Under agency policy, are there circumstances when a supervisor may direct the officer to record or not record?	no only to stop recording depending on situation.
5	What is the agency's policy regarding citizen notification of BWC recording?	no requirement to notify citizens
6	If the TFO's BWC is inoperable does the agency's policy permit the TFO to participate in enforcement activities if a replacement is not readily available?	yes but the incident must be documented.

E. Law Enforcement Access to BWC Recordings		
1	Are officers allowed to review BWC recordings before writing reports? Giving statements? <ul style="list-style-type: none"> If so, are they allowed to view only recordings from their own BWC, or are they allowed view BWC recordings from other officers? 	Yes they can review their recordings. Only supervisors can review others recordings. they can review but someone else must show them the recording.
2	If officers are allowed to review recordings are there any exceptions? If so list the exceptions, e.g., internal investigations, critical incidents (e.g., officer-involved shooting (OIS), use of deadly force, etc.)?	With an OIS they don't review until they have meet with their attorney.
3	Who in the parent agency will have access to TFOs' BWC recordings involving ATF/federal cases?	Admins, supervisors and evidence custodian.
4	Does agency restrict access to BWC recordings involving a critical incident (e.g., OIS)? If so, who has access in those situations?	no we do not restrict access unless there is a specific need.
5	Will members of the parent agency be able to identify ATF cases in the BWC system? How?	The TFO can "tag" the recording with relevant info
6	Does the agency require random or directed supervisory review/audit of officer videos for policy compliance or other issues? If so, will this include TFO recordings of ATF cases?	no requirement to audit recordings.
7	Will non-law enforcement employees of the parent agency or municipality have access to ATF BWC recordings, e.g., IT? If so, are they CJIS-compliant (e.g., CJIS background checks)?	The only no LE person with access are the two evidence custodians and IT person all have had a CJIS background checks.
8	Are officers allowed to make copies of BWC recordings, or must they obtain recordings from someone else within the agency?	They can download recordings.
9	Are officers allowed to possess copies of recordings outside the police facility, or retain possession of copies for personal use?	Not unless they submit a request just as any other citizen could.
10	Does the agency have a policy prohibiting sharing of recordings outside of law enforcement for non-official reasons?	Yes we do.
11	Does the agency have a policy prohibiting the posting of BWC recordings to the Internet, social media sites, or the media for non-official purposes?	yes we do.
12	Does the agency have a policy prohibiting officers from wearing or using privately owned BWCs or any other non-issued BWC?	yes we do.
13	Do any other law enforcement entities or personnel have direct access to recordings, e.g., prosecutor's office?	not at this time.

14	<p>Does the parent agency investigate TFO-involved shootings (or other TFO-involved events involving death or serious injury), or is this done by another agency? If another agency:</p> <ul style="list-style-type: none"> • Identify the agency. • Is there an agreement, policy, or protocol in place with the agency for handling these situations? If so, attach. 	<p>No we do not, NM State Police has done all of our OIS events. There is no written agreement for this.</p>
-----------	--	--

F. External Access to BWC Recordings		
1	<p>How does the agency handle external requests for BWC recordings?</p> <ul style="list-style-type: none"> • Criminal discovery, subpoenas? • Civil/administrative discovery, subpoenas? • Open record/freedom of information requests? • Media requests? • Union requests? Is there an agreement with the union regarding union disclosure of BWC recordings? If so, attach copy. 	<p>locate recording, asses if they have to pay, redact if required, and then sent recording.</p> <p>There is no union agreement for the recordings.</p>
2	<p>If the agency uses a 3rd party vendor to store recordings:</p> <ul style="list-style-type: none"> • is security of or access to recordings addressed in the contract? • are background checks of vendor employees addressed in the contract? <p>If so, attach copy.</p>	<p>Yes data stored on Microsoft Azure Government Cloud</p>
3	<p>How does the agency handle redaction of BWC recordings prior to public release?</p>	<p>yes we do.</p>

To: (b) (6), (b) (7)(C)]; Vanderplow, Paul D[(b) (6), (b) (7)(C)
(b) (6), (b) (7)(C)
From: (b) (6), (b) (7)(C)
Sent: Tue 8/24/2021 3:57:14 PM
Subject: Draft - **FMS NOTIFICATION MESSAGE - #21-0824.1 – PRIORITY: ROUTINE - Implementation of Federal Agent Body Worn Camera Policy**

Draft – Once approved, I will distribute.

***THIS MESSAGE AUTHORIZED BY THE CHIEF, FIELD MANAGEMENT
STAFF***

(b) (5)

(b) (5)

Should you have any questions as this effort progresses, please send them to (b) (2) [REDACTED]@atf.gov or contact Chief, Paul D. Vanderplow at (b) (6), (b) (7)(C).

To: (b) (6), (b) (7)(C)
From: (b) (6), (b) (7)(C)
Sent: Mon 8/9/2021 8:50:29 PM
Subject: Checklist
ATF Checklist Blank.pdf

Per your request...

(b) (6), (b) (7)(C)
Alcohol, Tobacco, Firearms and Explosives
16009 N. 81st Street, Suite 100
Scottsdale, AZ 85260
Special Agent Project Officer-Digital Evidence Management
Technical Project Office
Special Operations Division
(b) (6), (b) (7)(C)

CONFIDENTIALITY NOTICE: E-mail may contain confidential information that is legally privileged. Do not read this e-mail if you are not the intended recipient.

This e-mail transmission, and any documents, files or previous e-mail messages attached to it may contain confidential information that is legally privileged. If you are not the intended recipient, or a person responsible for delivering it to the intended recipient, you are hereby notified that any disclosure, copying, distribution or use of any of the information contained in or attached to this transmission is **STRICTLY PROHIBITED**. If you have received this transmission in error, please immediately notify us by reply e-mail, by forwarding this to (b) (6), (b) (7)(C) or by telephone at (b) (6), (b) (7)(C) and destroy the original transmission and its attachments without reading or saving in any manner. Thank you.

ATTACHMENT 1

Standard Operating Procedures for Task Force Officer Body-Worn Camera Program

BODY-WORN CAMERA TASK FORCE OFFICER AGENCY CHECKLIST

****Complete separate checklist for each agency employing task force officers that will use body-worn cameras (BWC). Attach additional sheets if necessary.****

Date: _____

ATF Division	Task Force	State/Local Agency
Person Completing Checklist		
Name	Phone Number	Email Address

A. State & Local Legal Authority		
List and attach any state or local laws applicable to BWCs or impacting BWCs (e.g., open records laws, legal retention requirements, etc.); and other pertinent legal guidance (e.g., significant case law, State AG Opinions, etc.). If none, enter "N/A." Add additional rows as necessary.		
Title	Cite	Comments
B. TFO Parent Agency Policies		
List and attach any policy, procedure, or other written directive from the TFO's parent agency applicable to TFOs' use of BWCs. Include any union or other labor agreement requirements regarding BWCs applicable to TFOs. If none, enter "N/A." Add additional rows as necessary.		
Title	Cite	Comments

Answer the following questions, including any applicable citation (e.g., state or local law, agency policy, vendor contract, etc.).

C. BWC System

1	Name/model of BWC used by agency? Attach technical specifications.	
2	Internal storage of recordings or external with a 3 rd party vendor? If a 3 rd party, identify the vendor, attach contract.	
3	Does the BWC system include a “buffer” or “pre-record” function, or a “post-record” function? If so, state the length of the buffer/pre-record and/or post-record, and whether it is audio only or both audio and video.	
4	Can the system be configured to give designated ATF personnel direct access to view and copy TFO recordings at the ATF office?	
5	Will ATF need specialized software or equipment to view recordings? If so, specify.	
6	Will ATF need specialized software or equipment to copy recordings? If so, specify.	
7	Does the system have an audit function that will identify persons who accessed, downloaded, or copied recordings?	
8	How will ATF cases be identified in the agency’s system?	
9	What metadata can be obtained from BWC recordings?	
10	How long will recordings be preserved in the agency’s system? Attach any agency retention schedule, and note whether it is mandated by state /local law or agency policy only.	
11	Does the BWC system allow restriction of BWC recording access to specific persons within the agency?	
12	How does agency handle inadvertent/accidental recordings?	
13	How does agency handle requests to delete BWC recordings?	
14	Will the TFO be able to charge the BWC and/or download/upload the recordings into the agency’s BWC system at the ATF task force office?	
15	Does the BWC have a GPS function? If so, is the function available to the TFO, and what is the agency’s policy regarding use of GPS? Can it be deactivated on TFO BWCs?	

16	Does the BWC have a “live stream” capability? If so, is the function available to the TFO, and what is the agency’s policy regarding use of “live streaming” with BWCs? Can it deactivated on TFO BWCs?	
17	Does the agency utilize facial recognition technology with BWC recordings?	
18	Provide an agency point-of-contact who can provide information regarding system security and protections, and location and security precautions of data storage facilities. <i>*Do not attach this information.*</i>	

<i>D. BWC Use</i>		
1	Are there any exceptions under agency policy to the requirement to record search warrant executions or arrests?	
2	What is the agency's policy regarding BWC recording of CSs?	
3	Does agency prohibit BWC recording in any specific situations? If so, list.	
4	Under agency policy, are there circumstances when a supervisor may direct the officer to record or not record?	
5	What is the agency's policy regarding citizen notification of BWC recording?	
6	If the TFO's BWC is inoperable does the agency's policy permit the TFO to participate in enforcement activities if a replacement is not readily available?	

<i>E. Law Enforcement Access to BWC Recordings</i>		
1	Are officers allowed to review BWC recordings before writing reports? Giving statements? <ul style="list-style-type: none"> If so, are they allowed to view only recordings from their own BWC, or are they allowed view BWC recordings from other officers? 	
2	If officers are allowed to review recordings are there any exceptions? If so list the exceptions, e.g., internal investigations, critical incidents (e.g., officer-involved shooting (OIS), use of deadly force, etc.)?	
3	Who in the parent agency will have access to TFOs' BWC recordings involving ATF/federal cases?	
4	Does agency restrict access to BWC recordings involving a critical incident (e.g., OIS)? If so, who has access in those situations?	
5	Will members of the parent agency be able to identify ATF cases in the BWC system? How?	
6	Does the agency require random or directed supervisory review/audit of officer videos for policy compliance or other issues? If so, will this include TFO recordings of ATF cases?	
7	Will non-law enforcement employees of the parent agency or municipality have access to ATF BWC recordings, e.g., IT? If so, are they CJIS-compliant (e.g., CJIS background checks)?	
8	Are officers allowed to make copies of BWC recordings, or must they obtain recordings from someone else within the agency?	
9	Are officers allowed to possess copies of recordings outside the police facility, or retain possession of copies for personal use?	
10	Does the agency have a policy prohibiting sharing of recordings outside of law enforcement for non-official reasons?	
11	Does the agency have a policy prohibiting the posting of BWC recordings to the Internet, social media sites, or the media for non-official purposes?	
12	Does the agency have a policy prohibiting officers from wearing or using privately owned BWCs or any other non-issued BWC?	
13	Do any other law enforcement entities or personnel have direct access to recordings, e.g., prosecutor's office?	

14	<p>Does the parent agency investigate TFO-involved shootings (or other TFO-involved events involving death or serious injury), or is this done by another agency? If another agency:</p> <ul style="list-style-type: none"> • Identify the agency. • Is there an agreement, policy, or protocol in place with the agency for handling these situations? If so, attach. 	
-----------	--	--

F. External Access to BWC Recordings

1	How does the agency handle external requests for BWC recordings? <ul style="list-style-type: none">• Criminal discovery, subpoenas?• Civil/administrative discovery, subpoenas?• Open record/freedom of information requests?• Media requests?• Union requests? Is there an agreement with the union regarding union disclosure of BWC recordings? If so, attach copy.	
2	If the agency uses a 3 rd party vendor to store recordings: <ul style="list-style-type: none">• is security of or access to recordings addressed in the contract?• are background checks of vendor employees addressed in the contract? If so, attach copy.	
3	How does the agency handle redaction of BWC recordings prior to public release?	

To: ATF - FO - SES - FIELD (b) (2) @atf.gov; ATF - FO - ASAC (b) (2) @atf.gov; ATF - FO - DOO (b) (2) @atf.gov
Cc: ATF - FO - SES - HQ (b) (2) @doj365.mail.onmicrosoft.com; FMS- ISB (b) (2) @atf.gov; FMS Notifications (b) (2) @atf.gov; (b) (6), (b) (7)(C) (b) (6), (b) (7)(C); Vanderplow, Paul D (b) (6), (b) (7)(C) (b) (6), (b) (7)(C) (b) (6), (b) (7)(C) (b) (6), (b) (7)(C) (b) (6), (b) (7)(C) (b) (6), (b) (7)(C)
From: (b) (6), (b) (7)(C)
Sent: Tue 8/24/2021 5:48:40 PM
Subject: **FMS NOTIFICATION MESSAGE - #21-0824.1 – PRIORITY: ROUTINE - Implementation of Federal Agent Body Worn Camera Policy**

THIS MESSAGE AUTHORIZED BY THE CHIEF, FIELD MANAGEMENT STAFF

On 01-Sep-21, ATF will be the first Department of Justice Agency to commence the Body Worn Camera (BWC) pilot program. The remaining DOJ entities will begin on or about 15-Sep-21.

In October 2019, at the direction of the Department of Justice (DOJ), ATF, along with other DOJ components, participated in a pilot program allowing Task Force Officers, (TFO) under specific parameters, to wear Body Worn Cameras (BWC) during federal planned arrest warrants or planned search warrants. Recognizing the ubiquitous nature of digital evidence, deemed federal record by DOJ, ATF SOD acquired, provided training, and ultimately implemented, a cloud based digital storage case management system, (Axon Evidence.com). In addition, ATF SOD established the Technical Project Office (TPO) to oversee the TFO BWC pilot.

In September 2020, the pilot concluded and on October 29, 2020, DOJ created a permanent policy allowing the use of body worn cameras by federally deputized Task Force Officers. This policy required all the DOJ components to maintain these BWC recordings, therefore, ATF SOD TPO established a Task Force Officer Body Worn Camera program, this program included;

- an addendum to the current TFO Memorandum of Understanding (MOU)
- acquisition of a cloud-based storage and case management system utilizing Axon Evidence.com
- TFO BWC program Standard Operating Procedures
- feedback surveys of the pilot ATF Field Divisions (Detroit, Houston, and Kansas City/Wichita)
- identification of all ATF Field Divisions affected by the new DOJ Policy
- assignment of administrative personnel for each affected division
- coordination of ATF TFO BWC program training and digital cloud storage service provider training for affected ATF Field Divisions
- restructuring of the TFO Joint Law Enforcement Operations (JLEO) onboarding process to address partner agency BWC policies
- coordination with the partner agencies to implement the addendum to the existing TFO MOU for those affected divisions

Most recently, the Office of the Deputy Attorney General (ODAG) has mandated the implementation of a federal agent BWC policy. SOD TPO has proposed a phased BWC agency implementation. Phase I, beginning on September 1, 2021, will assess the feasibility of a permanent ATF body-worn camera program. It will also identify any infrastructure shortcomings and assist in recognizing training

deficiencies. Each pilot division will provide feedback of the digital evidence platforms advantages and disadvantages. The proposed pilot locations, with the concurrence of the Assistant Director (Field Operations) and the Special Agent in Charge, (SAC) include the Detroit and Phoenix Field Divisions as well as the ATF National Academy. Agents within these field divisions, will wear BWC's during pre-planned law enforcement actions currently outlined in both the Department of Justice Use of Body-Worn Cameras Policy, ATF BWC Policy, and ATF Standard Operating Policy and Procedures. Upon conclusion of Phase I, an in-depth review will be conducted utilizing feedback from the participating divisions and other ATF directorates to begin an agency-wide implementation, if and when additional funding is provided.

Should you have any questions as this effort progresses, please send them to (b) (2) [REDACTED]@atf.gov or contact Chief, Paul D. Vanderplow at (b) (6), (b) (7)(C) [REDACTED]

To: Vanderplow, Paul D (b) (6), (b) (7)(C)
From: Braverman, Adam L. (ODAG)
Sent: Sat 7/24/2021 1:57:11 AM
Subject: FW: ATF – DEM – SOP – 20-0113.1443 ATF Policy Revisions
ATF - DEM - BWC - SOP - 21-07-22 Draft.docx

Hi Paul
Please let me know when you have a minute to discuss.
Thanks
Adam

From: (b) (6), (b) (7)(C)
Sent: Friday, July 23, 2021 3:38 PM
To: Braverman, Adam L. (ODAG) <Adam.L.Braverman@usdoj.gov>
Subject: ATF – DEM – SOP – 20-0113.1443 ATF Policy Revisions

Sir,

I have spoken to Chief Vanderplow regarding the proposed ATF BWC Policy changes. Based on his many years of experience in ATF, many of which specifically developing various agency policies, he would prefer to leave the document as is at this time.

I have attached the **DRAFT** of the ATF BWC Standard Operating Procedures. This ATF SOP will eventually encompass all the agencies digital evidence management therefore the first section (2.0-2.0.13, Appendix A-D, Attachment 1) all pertain to the TFO BWC program. The ATF BWC Policy begins on page 38 and includes Appendix E-H, (G,H are not yet included).

(b) (6), (b) (7)(C)
Alcohol, Tobacco, Firearms and Explosives
16009 N. 81st Street, Suite 100
Scottsdale, AZ 85260
Special Agent Project Officer-Digital Evidence Management
Technical Project Office
Special Operations Division
(b) (6), (b) (7)(C)

CONFIDENTIALITY NOTICE: E-mail may contain confidential information that is legally privileged. Do not read this e-mail if you are not the intended recipient.

This e-mail transmission, and any documents, files or previous e-mail messages attached to it may contain confidential information that is legally privileged. If you are not the intended recipient, or a person responsible for delivering it to the intended recipient, you are hereby notified that any disclosure, copying, distribution or use of any of the information contained in or attached to this transmission is **STRICTLY PROHIBITED**. If you have received this transmission in error, please immediately notify us by reply e-mail, by forwarding this to (b) (6), (b) (7)(C) or by telephone at (b) (6), (b) (7)(C) and destroy the original transmission and its attachments without reading or saving in any manner. Thank you.



BUREAU OF ALCOHOL, TOBACCO, FIREARMS AND EXPLOSIVES

STANDARD OPERATING PROCEDURES FOR

DIGITAL EVIDENCE MANAGEMENT

TABLE OF CONTENTS

(b) (5)

(b) (5)

Appendix A: *Department of Justice Policy on Use of Body-Worn Cameras by Federally Deputized Task Force Officers*

Appendix B: *List of Acronyms Used*

Appendix C: *Addendum to Task Force Agreements Pertaining to Body Worn Cameras and Checklist (Attachment 1)*

Appendix D: *Agency Policy Memo-TBD*

Appendix E: *Memorandum from Deputy Attorney General Lisa Monaco, Body-Worn Camera Policy*

Appendix F: *ATF BWC Categories*

Appendix G: *List of Acronyms Used*

Appendix H: *Photograph of Body-Worn Camera Placement-Front*

Appendix I: *Photograph of Body-Worn Camera Placement-Helmet*

(b) (5)

(b) (5)

This document and its contents are the property of the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and may not be disseminated outside ATF (or if loaned outside of ATF, further disseminated) without the express written permission of the Office of Chief Counsel.

(b) (5)

This document and its contents are the property of the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and may not be disseminated outside ATF (or if loaned outside of ATF, further disseminated) without the express written permission of the Office of Chief Counsel.

(b) (5)

This document and its contents are the property of the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and may not be disseminated outside ATF (or if loaned outside of ATF, further disseminated) without the express written permission of the Office of Chief Counsel.

(b) (5)

This document and its contents are the property of the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and may not be disseminated outside ATF (or if loaned outside of ATF, further disseminated) without the express written permission of the Office of Chief Counsel.

(b) (5)

This document and its contents are the property of the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and may not be disseminated outside ATF (or if loaned outside of ATF, further disseminated) without the express written permission of the Office of Chief Counsel.

(b) (5)

This document and its contents are the property of the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and may not be disseminated outside ATF (or if loaned outside of ATF, further disseminated) without the express written permission of the Office of Chief Counsel.

(b) (5)

This document and its contents are the property of the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and may not be disseminated outside ATF (or if loaned outside of ATF, further disseminated) without the express written permission of the Office of Chief Counsel.

(b) (5)

This document and its contents are the property of the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and may not be disseminated outside ATF (or if loaned outside of ATF, further disseminated) without the express written permission of the Office of Chief Counsel.

(b) (5)

This document and its contents are the property of the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and may not be disseminated outside ATF (or if loaned outside of ATF, further disseminated) without the express written permission of the Office of Chief Counsel.

(b) (5)

This document and its contents are the property of the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and may not be disseminated outside ATF (or if loaned outside of ATF, further disseminated) without the express written permission of the Office of Chief Counsel.

(b) (5)

This document and its contents are the property of the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and may not be disseminated outside ATF (or if loaned outside of ATF, further disseminated) without the express written permission of the Office of Chief Counsel.

(b) (5)

This document and its contents are the property of the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and may not be disseminated outside ATF (or if loaned outside of ATF, further disseminated) without the express written permission of the Office of Chief Counsel.

(b) (5)

This document and its contents are the property of the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and may not be disseminated outside ATF (or if loaned outside of ATF, further disseminated) without the express written permission of the Office of Chief Counsel.

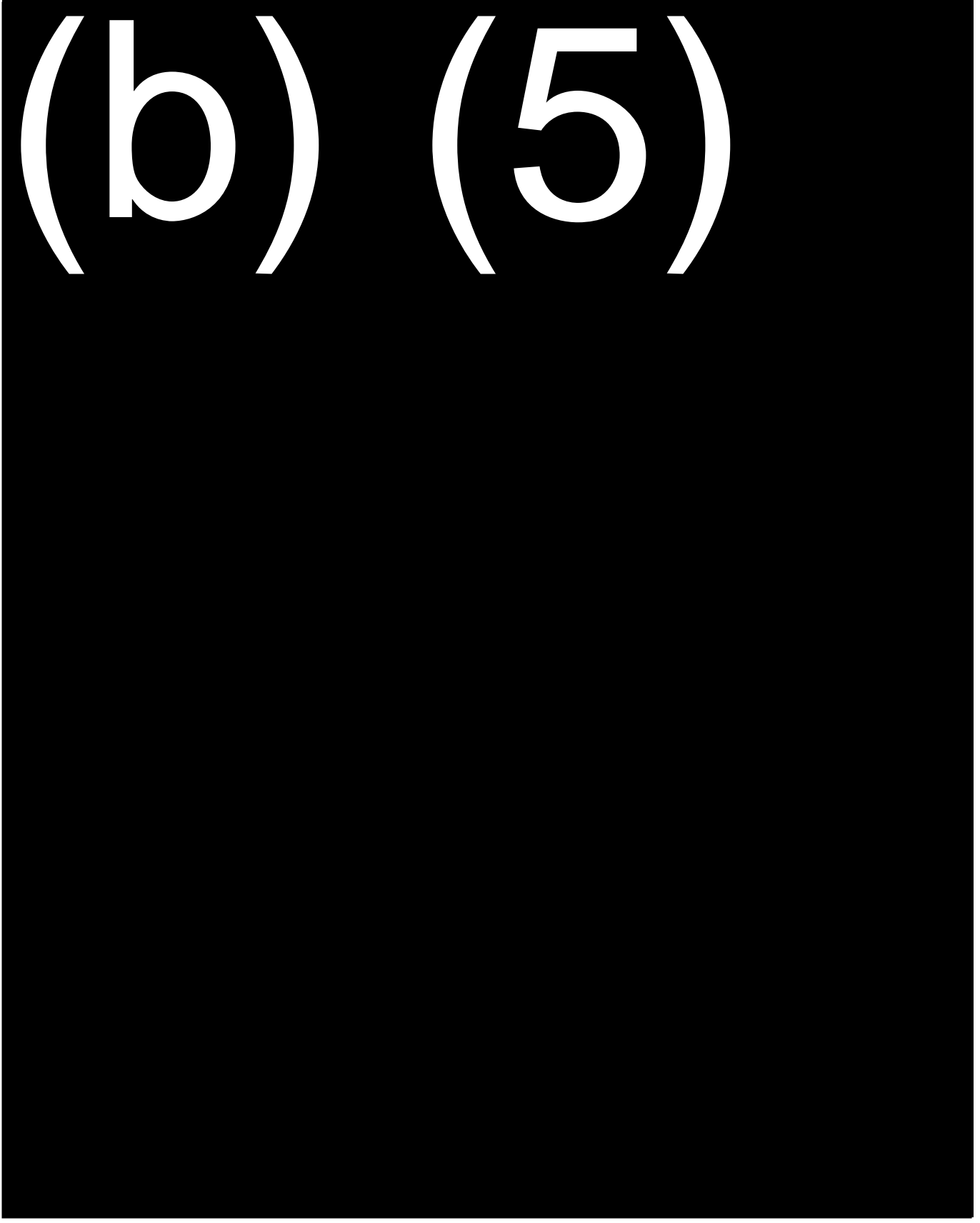
(b) (5)

This document and its contents are the property of the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and may not be disseminated outside ATF (or if loaned outside of ATF, further disseminated) without the express written permission of the Office of Chief Counsel.

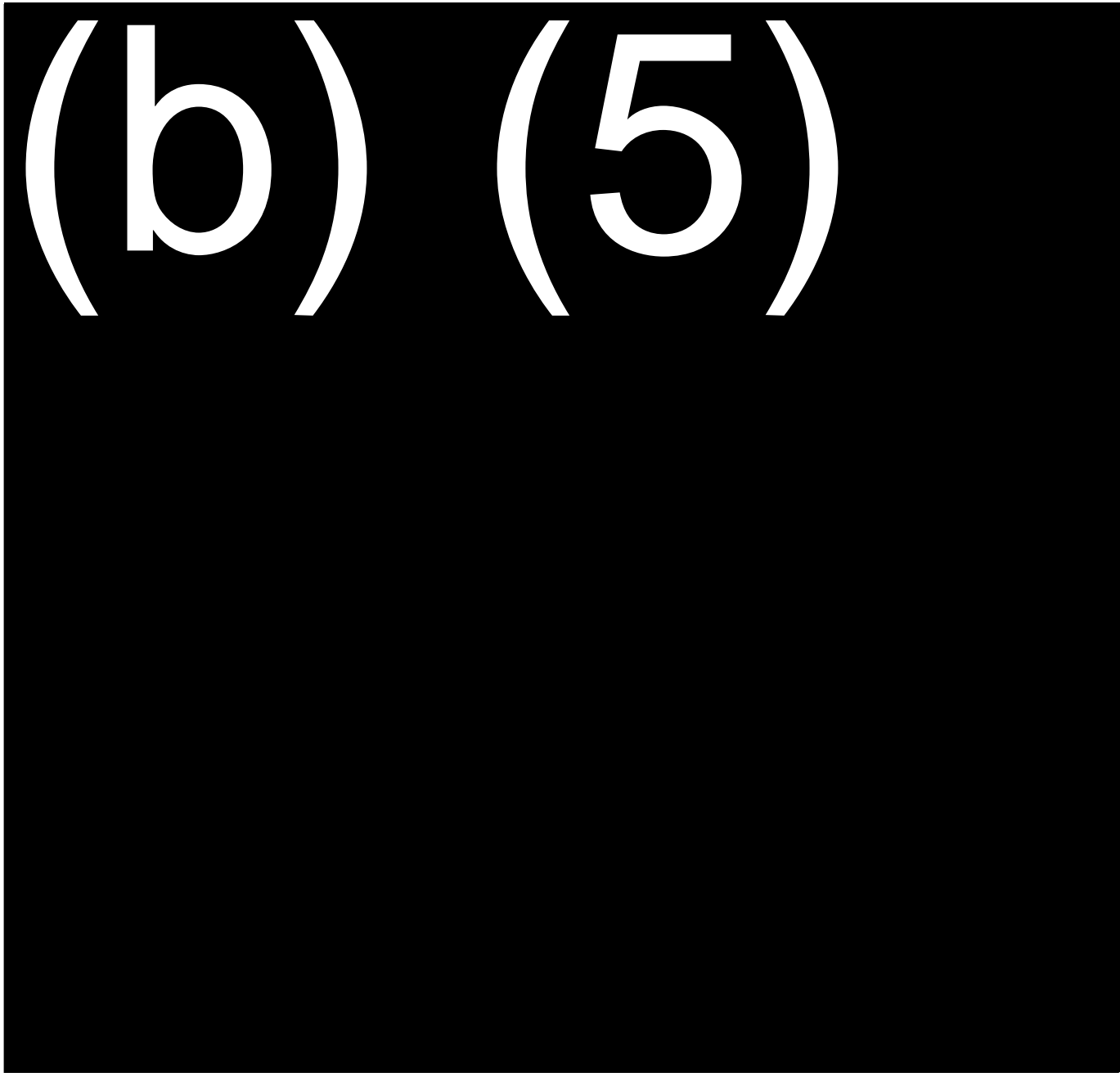
(b) (5)

This document and its contents are the property of the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and may not be disseminated outside ATF (or if loaned outside of ATF, further disseminated) without the express written permission of the Office of Chief Counsel.

(b) (5)



(b) (5)



APPENDIX

A

**Department of Justice Policy on Use of
Body-Worn Cameras by Federally
Deputized Task**

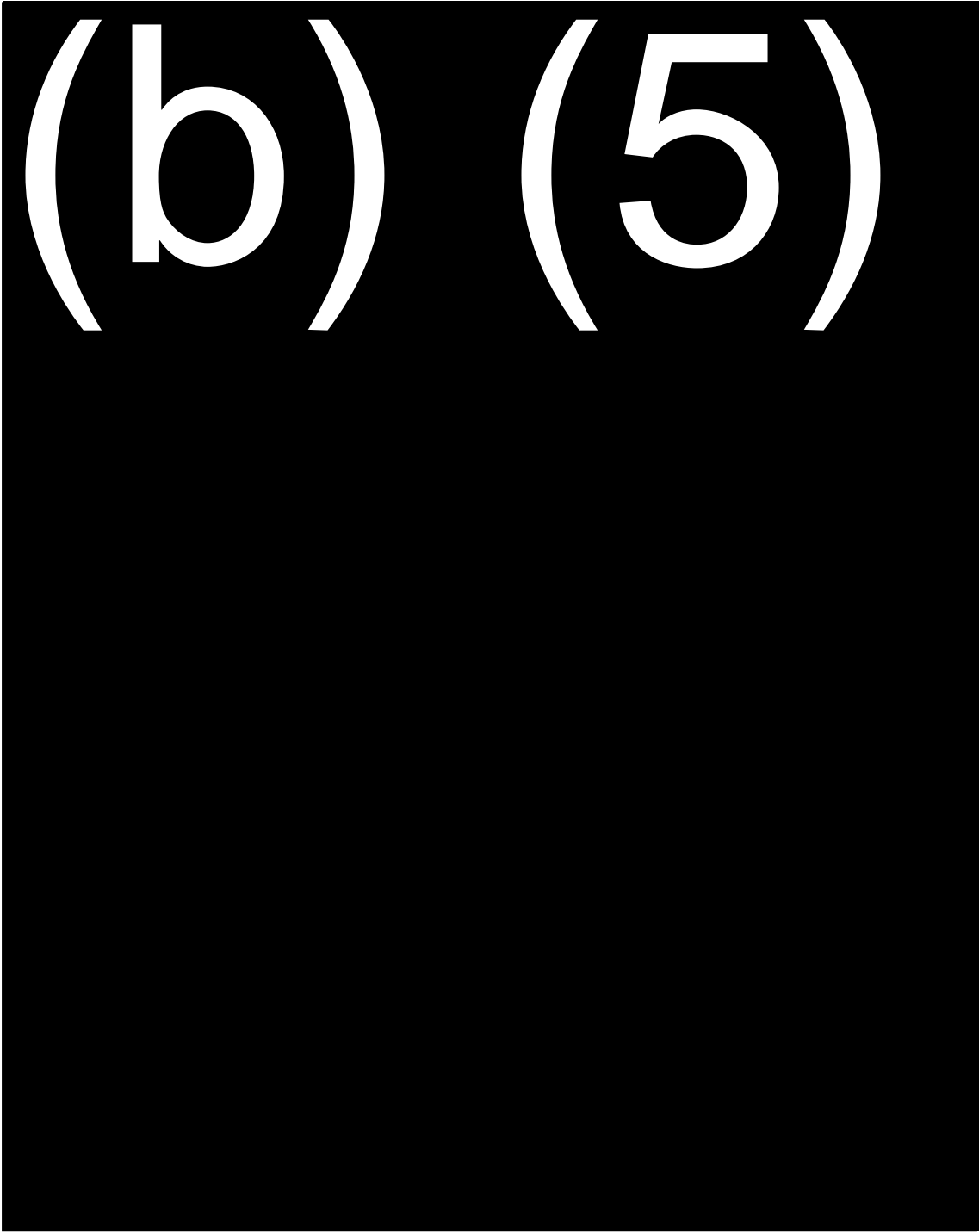


U.S. Department of Justice
Washington, D.C.

**USE OF BODY-WORN CAMERAS BY FEDERALLY DEPUTIZED
TASK FORCE OFFICERS**

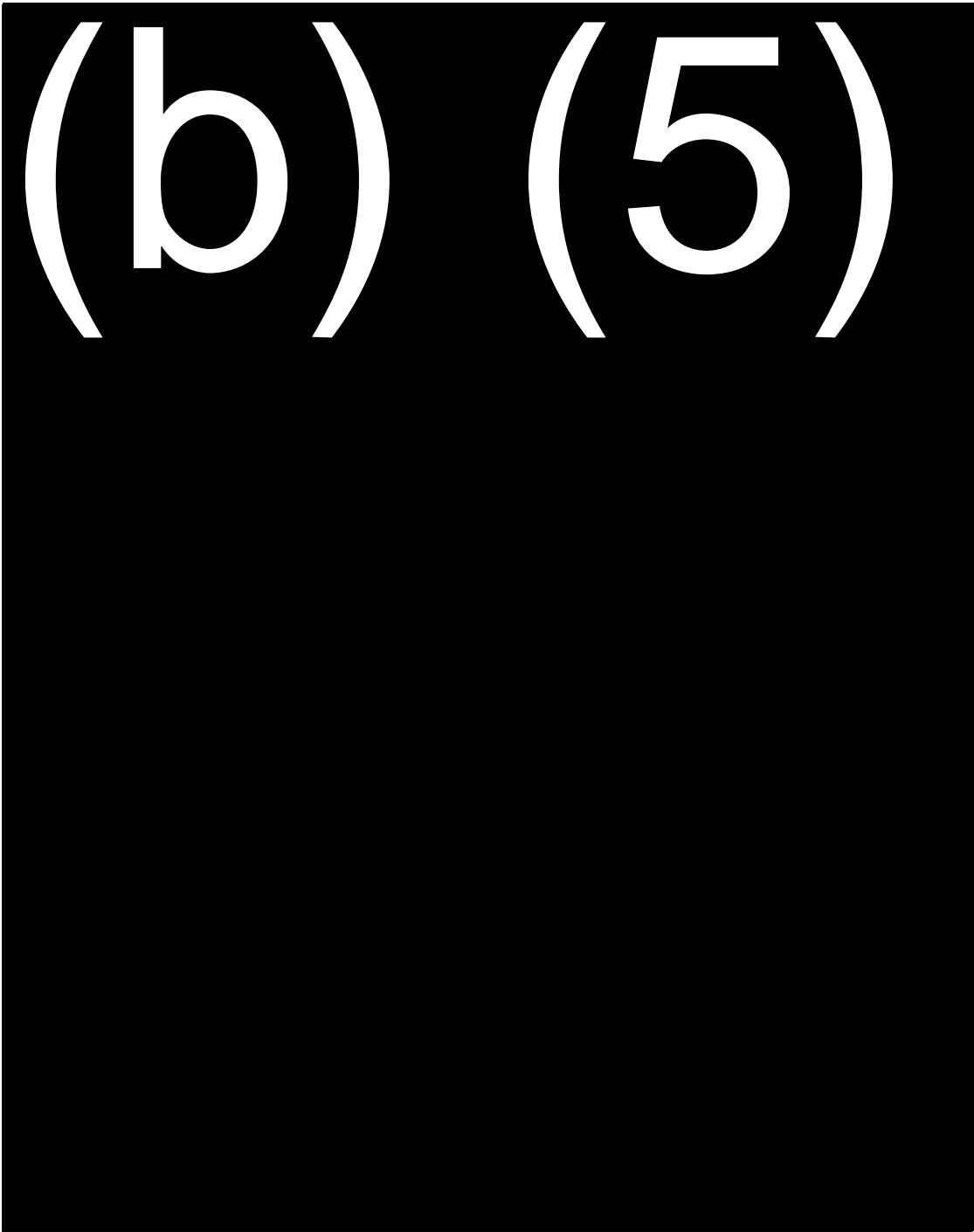
(b) (5)

(b) (5)

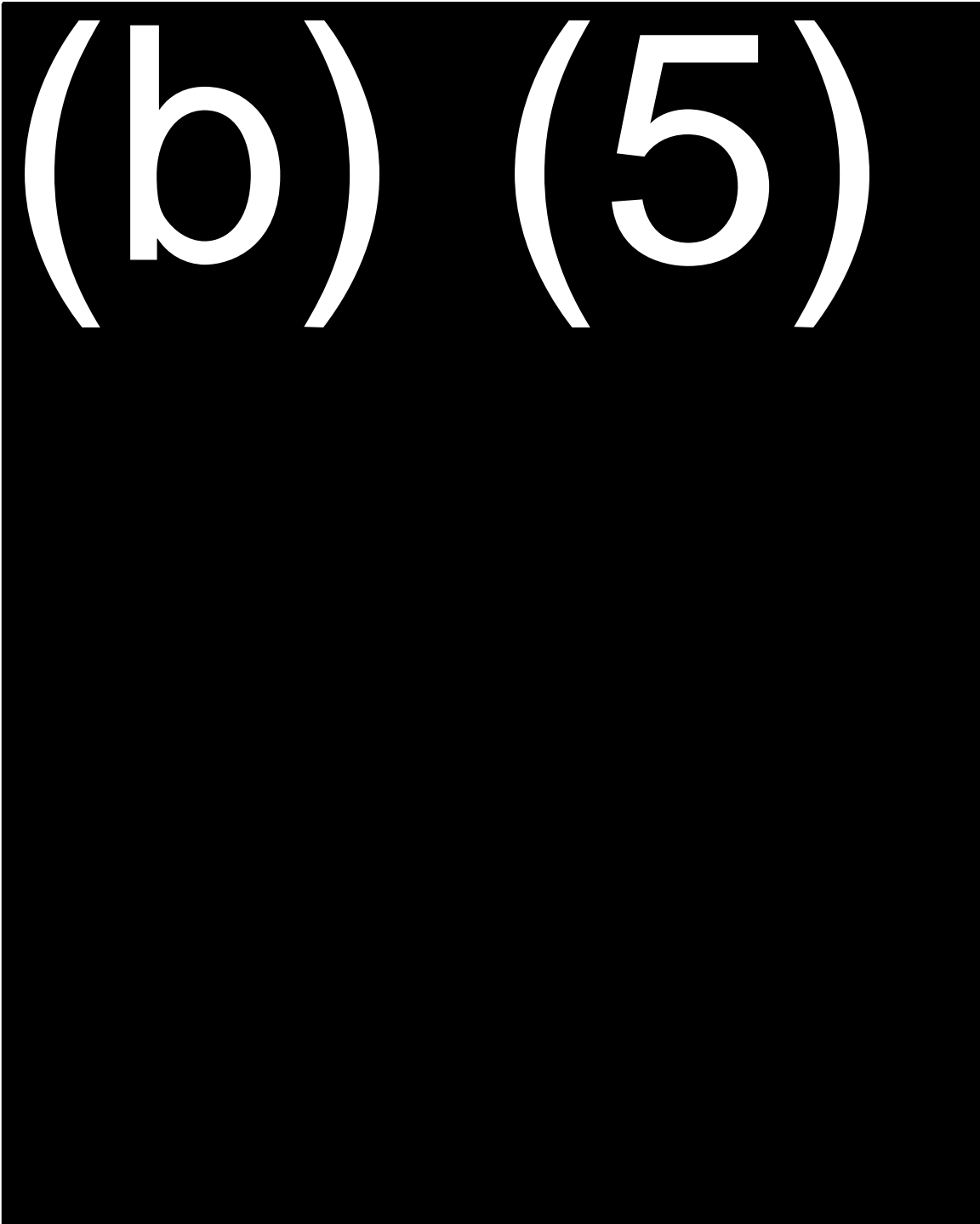


(b) (5)

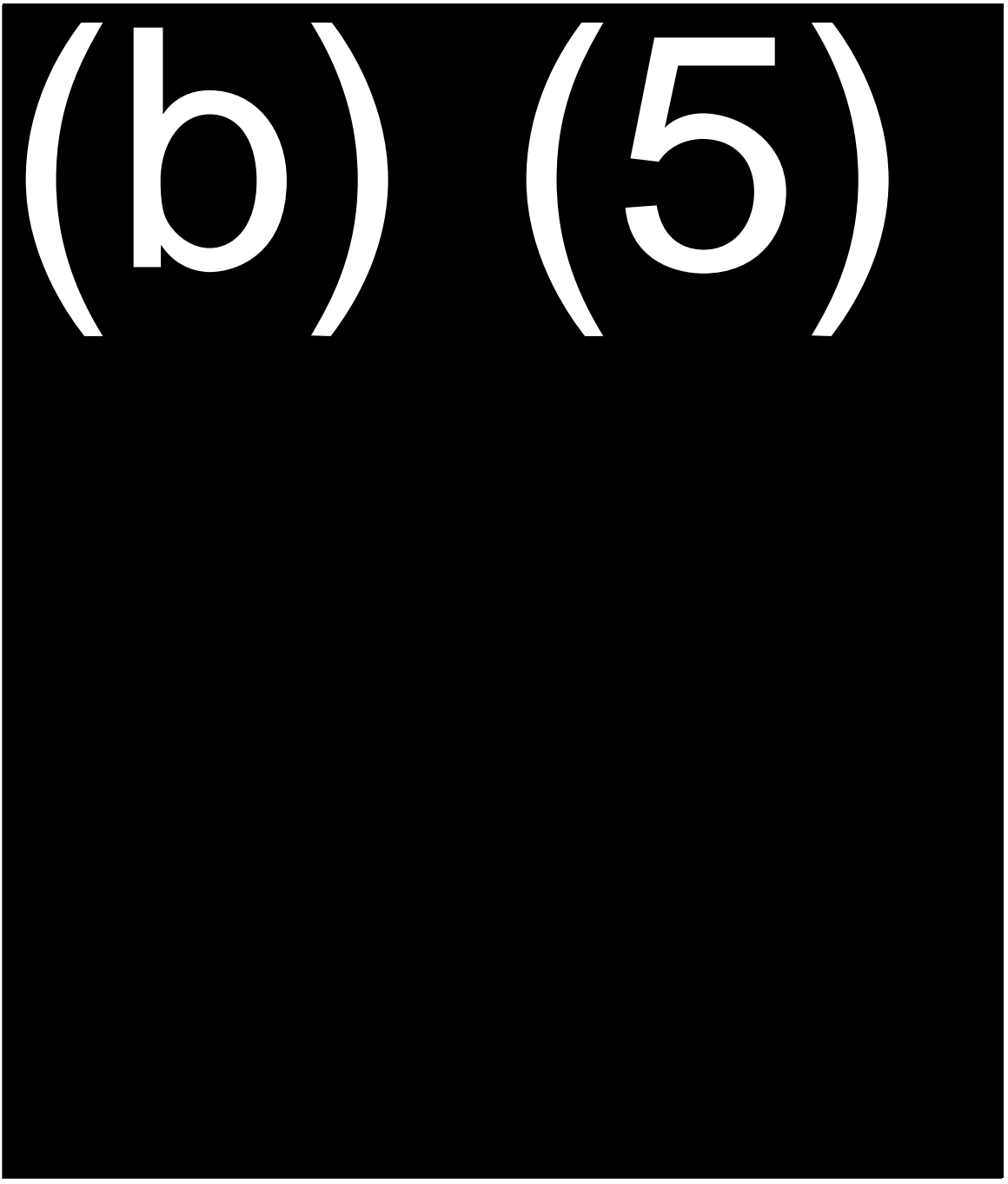
(b) (5)



(b) (5)



(b) (5)



APPENDIX B
Acronyms

ASAC	Assistant Special Agent in Charge
ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
BWC	Body-Worn Camera
CC	Office of Chief Counsel
CS	Confidential Source
DAD	Deputy Assistant Director
DFB	Digital Forensics Branch
DOJ	Department of Justice
FMS	Field Management Staff
FO	Office of Field Operations
FRO	Force Review Office
KEP	Kinetic Energy Projectile
OPRSO	Office of Professional Responsibility and Security Operations
OSII	Office of Strategic Intelligence and Information
OST	Office of Science and Technology
SA	Special Agent
SAC	Special Agent in Charge
SES	Senior Executive Service
SOD	Special Operations Division
SOP	Standard Operating Procedure
SSA	Supervisory Special Agent
SSD	Solid State Drives
TFO	Task Force Officer
TOB	Technical Operations Branch
UC	Undercover
USAO	United States Attorney's Office

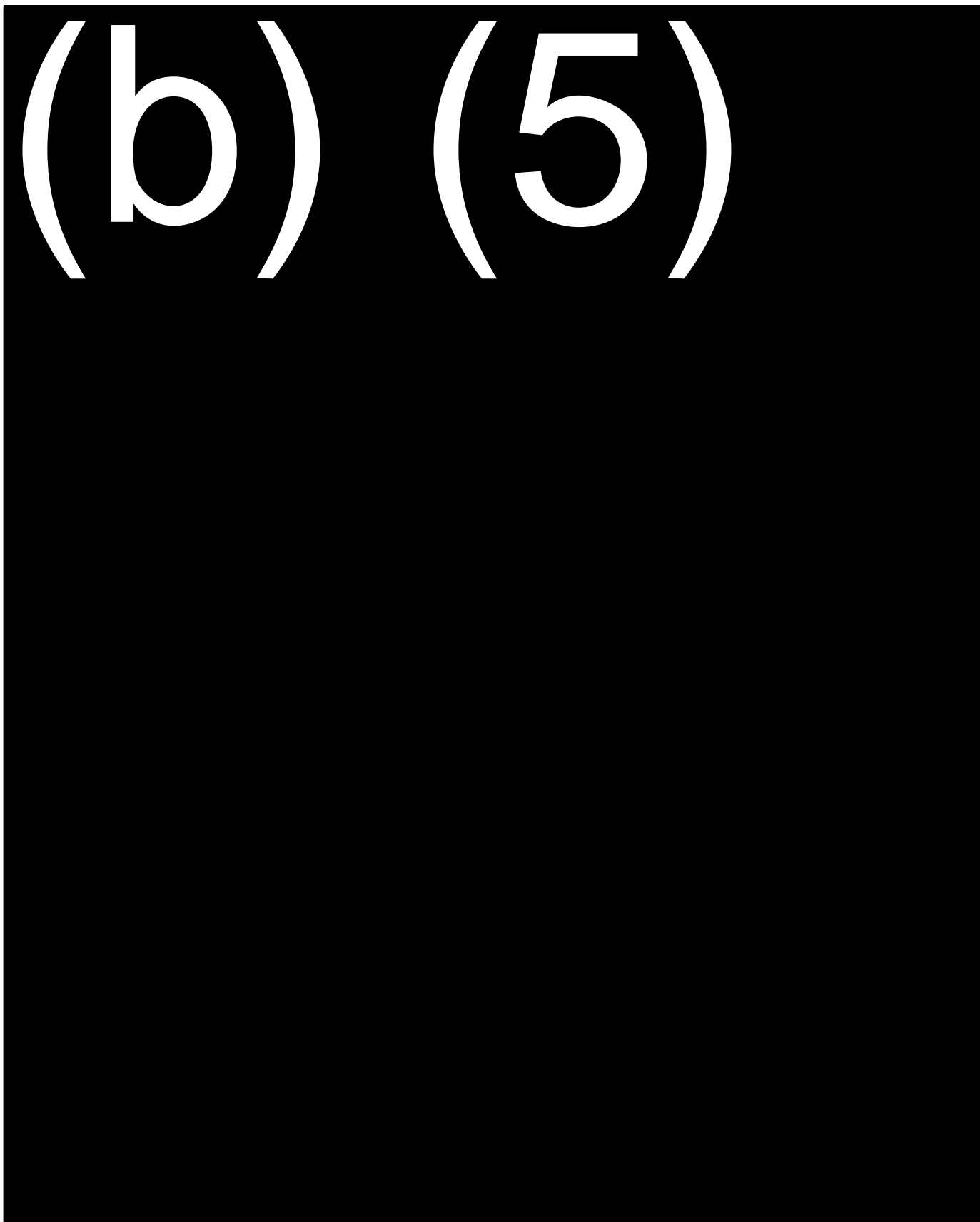
APPENDIX C

**ADDENDUM TO TASK FORCE AGREEMENTS PERTAINING TO BODY-WORN
CAMERAS**

(b) (5)

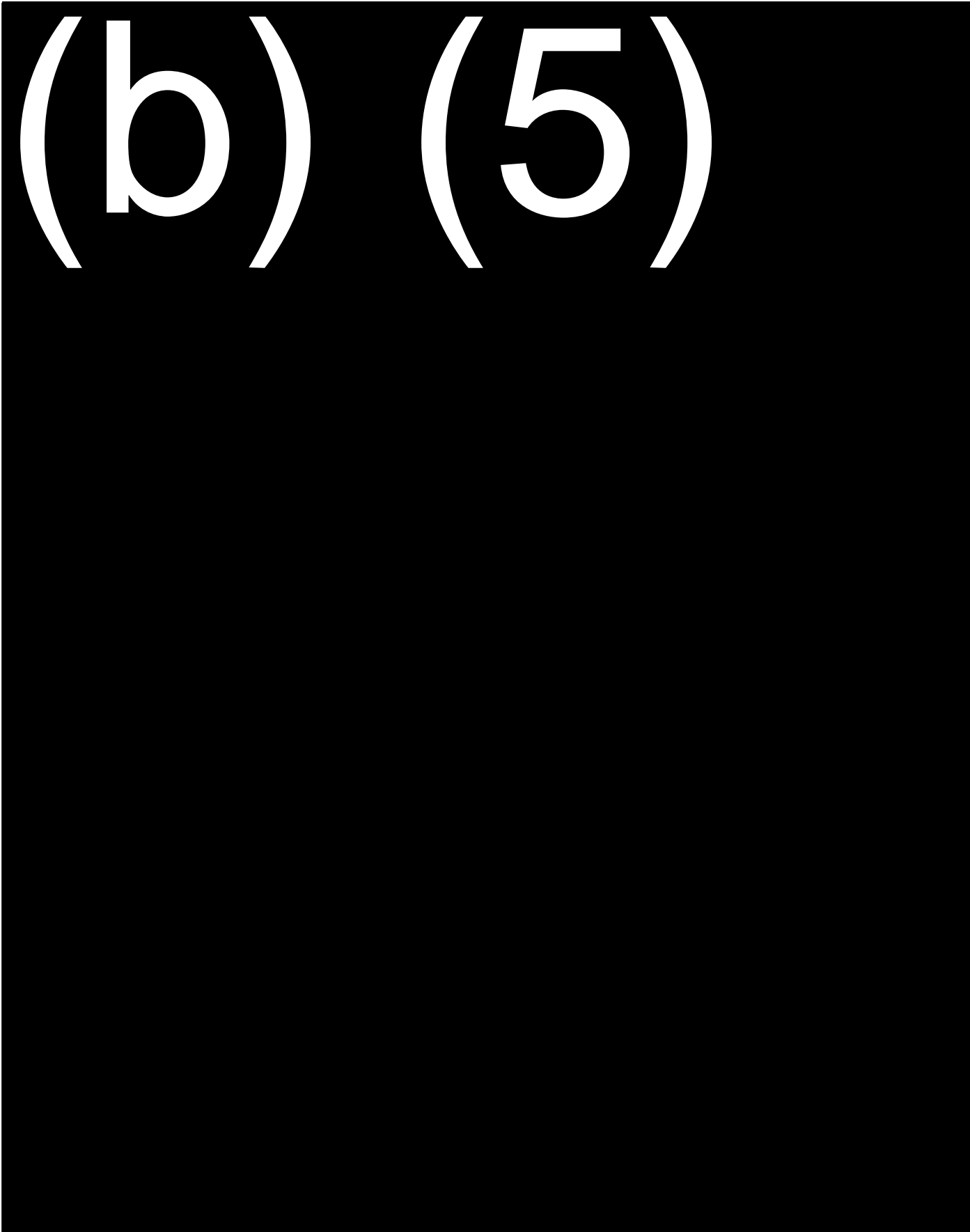
(b) (5)

(b) (5)



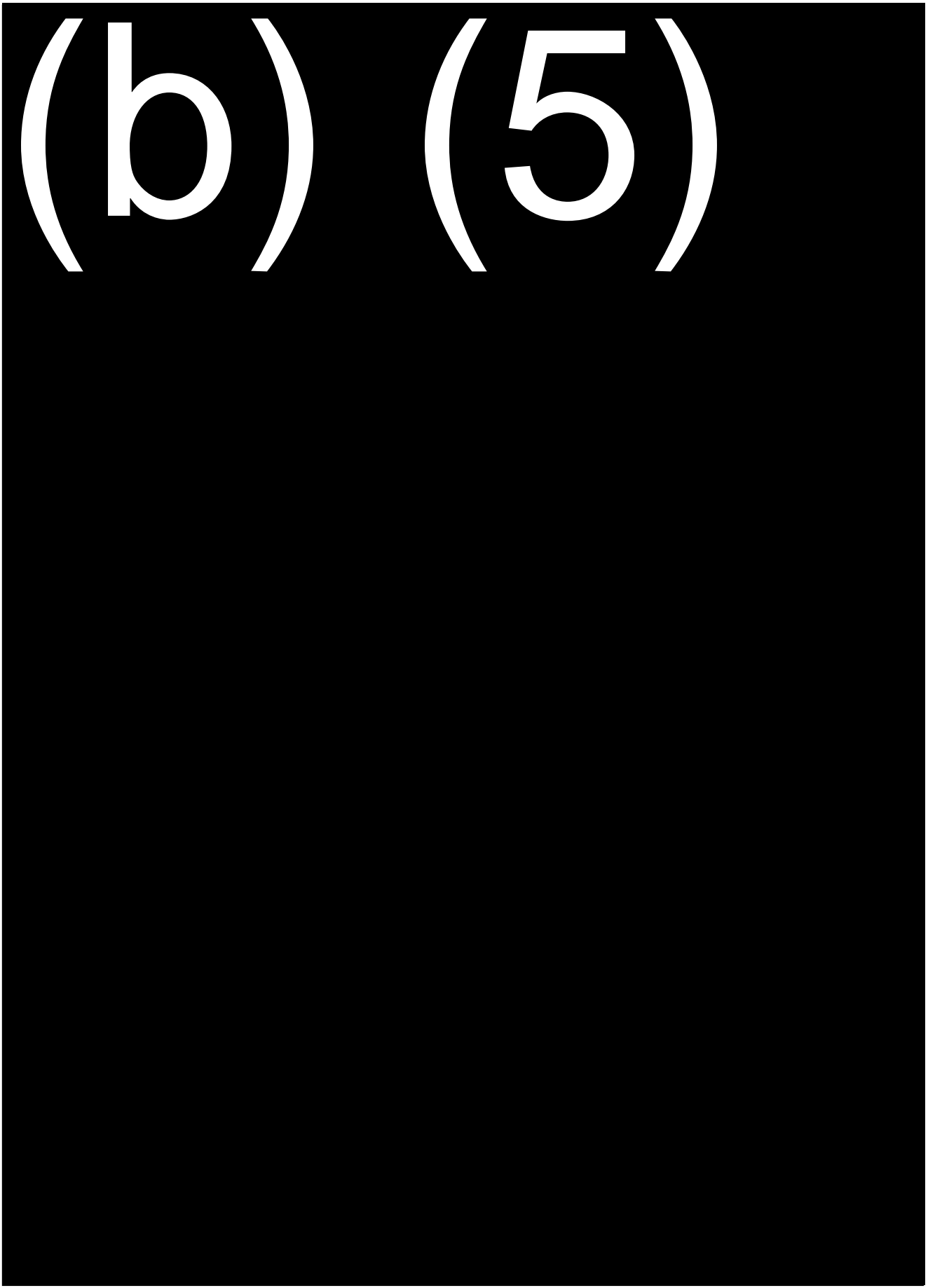
(b) (5)

(b) (5)



(b) (5)

(b) (5)



(b) (5)

APPENDIX D
Agency Policy Memo-TBD

ATTACHMENT 1

BODY-WORN CAMERA TASK FORCE OFFICER AGENCY CHECKLIST

Complete separate checklist for each agency employing task force officers that will use body-worn cameras (BWC). Attach additional sheets if necessary.

Date: _____

ATF Division	Task Force	State/Local Agency
Person Completing Checklist		
Name	Phone Number	Email Address

A. State & Local Legal Authority		
List and attach any state or local laws applicable to BWCs or impacting BWCs (e.g., open records laws, legal retention requirements, etc.); and other pertinent legal guidance (e.g., significant case law, State AG Opinions, etc.). If none, enter "N/A." Add additional rows as necessary.		
Title	Cite	Comments
B. TFO Parent Agency Policies		
List and attach any policy, procedure, or other written directive from the TFO's parent agency applicable to TFOs' use of BWCs. Include any union or other labor agreement requirements regarding BWCs applicable to TFOs. If none, enter "N/A." Add additional rows as necessary.		
Title	Cite	Comments

Answer the following questions, including any applicable citation (e.g., state or local law, agency policy, vendor contract, etc.).		
<i>C. BWC System</i>		
1	Name/model of BWC used by agency? Attach technical specifications.	
2	Internal storage of recordings or external with a 3 rd party vendor? If a 3 rd party, identify the vendor, attach contract.	
3	Does the BWC system include a “buffer” or “pre-record” function, or a “post-record” function? If so, state the length of the buffer/pre-record and/or post-record, and whether it is audio only or both audio and video.	
4	Will the TFO have access to download the BWC data at the ATF Office or will an administrator be required to provide to ATF?	
5	Can the system be configured to give designated ATF personnel direct access to view and copy TFO recordings at the ATF office?	
6	Will ATF need specialized software or equipment to view recordings? If so, specify.	
7	Will ATF need specialized software or equipment to copy recordings? If so, specify.	
8	Does the system have an audit function that will identify persons who accessed, downloaded, or copied recordings?	
9	How will ATF cases be identified in the agency’s system?	
10	What metadata can be obtained from BWC recordings?	
11	How long will recordings be preserved in the agency’s system? Attach any agency retention schedule, and note whether it is mandated by state /local law or agency policy only.	
12	Does the BWC system allow restriction of BWC recording access to specific persons within the agency?	
13	How does agency handle inadvertent/accidental recordings?	
14	How does agency handle requests to delete BWC recordings?	
15	Will the TFO be able to charge the BWC at the ATF task force office?	

16	Does the BWC have a GPS function? If so, is the function available to the TFO, and what is the agency's policy regarding use of GPS? Can it be deactivated on TFO BWCs?	
17	Does the BWC have a "live stream" capability? If so, is the function available to the TFO, and what is the agency's policy regarding use of "live streaming" with BWCs? Can it be deactivated on TFO BWCs?	
18	Does the agency utilize facial recognition technology with BWC recordings?	
19	Provide an agency point-of-contact who can provide information regarding system security and protections, and location and security precautions of data storage facilities. <i>*Do not attach this information.*</i>	
<i>D. BWC Use</i>		
1	Are there any exceptions under agency policy to the requirement to record search warrant executions or arrests?	
2	What is the agency's policy regarding BWC recording of CSs?	
3	Does agency prohibit BWC recording in any specific situations? If so, list.	
4	Under agency policy, are there circumstances when a supervisor may direct the officer to record or not record?	
5	What is the agency's policy regarding citizen notification of BWC recording?	
6	If the TFO's BWC is inoperable does the agency's policy permit the TFO to participate in enforcement activities if a replacement is not readily available?	

<i>E. Law Enforcement Access to BWC Recordings</i>		
1	Are officers allowed to review BWC recordings before writing reports? Giving statements? <ul style="list-style-type: none"> If so, are they allowed to view only recordings from their own BWC, or are they allowed view BWC recordings from other officers? 	
2	If officers are allowed to review recordings are there any exceptions? If so list the exceptions, e.g., internal investigations, critical incidents (e.g., officer-involved shooting (OIS), use of deadly force, etc.)?	
3	Who in the parent agency will have access to TFOs' BWC recordings involving ATF/federal cases?	
4	Does agency restrict access to BWC recordings involving a critical incident (e.g., OIS)? If so, who has access in those situations?	
5	Will members of the parent agency be able to identify ATF cases in the BWC system? How?	
6	Does the agency require random or directed supervisory review/audit of officer videos for policy compliance or other issues? If so, will this include TFO recordings of ATF cases?	
7	Will non-law enforcement employees of the parent agency or municipality have access to ATF BWC recordings, e.g., IT? If so, are they CJIS-compliant (e.g., CJIS background checks)?	
8	Are officers allowed to make copies of BWC recordings, or must they obtain recordings from someone else within the agency?	
9	Are officers allowed to possess copies of recordings outside the police facility, or retain possession of copies for personal use?	
10	Does the agency have a policy prohibiting sharing of recordings outside of law enforcement for non-official reasons?	
11	Does the agency have a policy prohibiting the posting of BWC recordings to the Internet, social media sites, or the media for non-official purposes?	
12	Does the agency have a policy prohibiting officers from wearing or using privately owned BWCs or any other non-issued BWC?	

13	Do any other law enforcement entities or personnel have direct access to recordings, e.g., prosecutor's office?	
----	---	--

14	Does the parent agency investigate TFO-involved shootings (or other TFO-involved events involving death or serious injury), or is this done by another agency? If another agency: <ul style="list-style-type: none"> • Identify the agency. • Is there an agreement, policy, or protocol in place with the agency for handling these situations? If so, attach. 	
<i>F. External Access to BWC Recordings</i>		
1	How does the agency handle external requests for BWC recordings? <ul style="list-style-type: none"> • Criminal discovery, subpoenas? • Civil/administrative discovery, subpoenas? • Open record/freedom of information requests? • Media requests? • Union requests? Is there an agreement with the union regarding union disclosure of BWC recordings? If so, attach copy. 	
2	If the agency uses a 3 rd party vendor to store recordings: <ul style="list-style-type: none"> • is security of or access to recordings addressed in the contract? • are background checks of vendor employees addressed in the contract? If so, attach copy.	
3	How does the agency handle redaction of BWC recordings prior to public release?	

APPENDIX E



U.S. Department of Justice
Office of the Deputy Attorney General

The Deputy Attorney General

Washington, D.C. 20530
June 7, 2021

MEMORANDUM FOR ACTING DIRECTOR, BUREAU OF ALCOHOL, TOBACCO,
FIREARMS & EXPLOSIVES
ACTING ADMINISTRATOR, DRUG ENFORCEMENT
ADMINISTRATION
DIRECTOR, FEDERAL BUREAU OF INVESTIGATION
DIRECTOR, UNITED STATES MARSHALS SERVICE
ASSISTANT ATTORNEY GENERAL FOR
ADMINISTRATION
EXECUTIVE OFFICE FOR UNITED STATES ATTORNEYS

FROM: THE DEPUTY ATTORNEY GENERAL *via Memo*

SUBJECT: BODY-WORN CAMERA POLICY

The Department of Justice recognizes that transparency and accountability in law enforcement operations build trust with the communities we serve. Although the Department's law enforcement components do not regularly conduct patrols or routinely engage with the public in response to emergency calls, there are circumstances where the Department's agents encounter the public during pre-planned law enforcement operations. The Department is committed to the use of body-worn cameras (BWCs) by the Department's law enforcement agents in such circumstances.

In October 2020, the Department announced a policy that permits state and local officers on Department of Justice Task Forces to wear and activate BWCs when the use of force is possible – while serving arrest warrants, executing other planned arrest operations, and during the execution of search warrants. Today, based on recommendations from the Department's law enforcement components, I am directing the Acting Director of the Bureau of Alcohol, Tobacco, Firearms & Explosives; the Acting Administrator of the Drug Enforcement Administration; the Director of the Federal Bureau of Investigation, and the Director of the United States Marshals Service to develop and submit for review, within 30 days, component BWC policies that require agents to wear and activate BWC recording equipment for purposes of recording their actions during: (1) a pre-planned attempt to serve an arrest warrant or other pre-planned arrest, including the apprehension of fugitives sought on state and local warrants; or (2) the execution of a search or seizure warrant or order.

Memorandum from the Deputy Attorney General
 Subject: Body-Worn Camera Policy

Page 2

Each law enforcement component shall develop its policy and a phased implementation plan for compliance with the above directive no later than 30 days from the date of this memorandum, and shall designate a senior official with responsibility for implementation and oversight of its BWC policy. Each component also shall ensure immediately that partners serving on DOJ-sponsored task forces are aware of the current Department policy that permits state and local officers on DOJ task forces to wear and activate BWCs.

Each component's BWC policy shall include:

- the responsibilities for Department agents to carry, operate, maintain, and secure the equipment, including when to activate and deactivate BWCs;
- the type(s) of BWC equipment authorized for use;
- the duration of time and scope of the BWC footage preserved prior to its activation (i.e., buffering period);
- specialized or sensitive investigative techniques or equipment that may require different treatment under the BWC policy;
- procedures governing the collection, storage, access, retention, use, and dissemination of BWC recordings, consistent with applicable federal laws;
- procedures governing the use of BWCs by all members of Department-sponsored task forces; and
- procedures for the expedited public release of recordings in cases involving serious bodily injury or death.

In addition, as soon as practicable, each component shall:

- submit for the approval of the Department's Chief Privacy and Civil Liberties Officer a Privacy Impact Assessment of the component's planned use of BWCs and associated equipment prior to implementation of its BWC policy, and a plan for annual privacy reviews;
- consult with the Office of Records Management to ensure the component's BWC policy is fully compliant with all records-related laws, regulations, rules, policies, and guidance;
- work with the Justice Management Division to assess resource requirements to fully implement its BWC policy and build upon the resources allocated to the Department to support BWC usage in FY22; and
- design evaluation metrics that can be used to measure the impact of its BWC policy.

Memorandum from the Deputy Attorney General
Subject: Body-Worn Camera Policy

Page 3

Finally, within 90 days, the Executive Office for U.S. Attorneys should develop training for prosecutors regarding the use of BWC recordings as evidence, building on existing trainings related to the discovery implications of these recordings.

I am proud of the job performed by the Department's law enforcement agents, and I am confident that these policies will continue to engender the trust and confidence of the American people in the work of the Department of Justice.

APPENDIX F

Category	Description
ATF Special Agent BWC	Default category that should be selected for every SA BWC recording
ATF Task Force Officer (TFO) BWC	Default category that should be selected for every ATF TFO BWC recording
Use of Force – Shooting (ATF)	Selection for video that includes firearm discharge by a ATF employee
Use of Force – Shooting (TFO)	Selection for video that includes firearm discharge by a Task Force Officer
Use of Force – Other (ATF)	Selection for video that includes non-firearm use by an ATF employee (CEW, etc)
Use of Force – Other (TFO)	Selection for video that includes non-firearm use by a Task Force Officer (CEW, etc)
Use of Force – K9 Bite	Selection for video that includes a K9 bite
Serious Injury/Death to Personnel (ATF/TFO)	Selection for video that includes injury or death of either ATF employees or Task Force Officers
Serious Injury/Death to Subject	Selection for video that includes injury or death of the subject of pre-planned arrest warrant or pre-planned search warrant
Serious Injury/Death to Other	Selection for video that includes injury or death of another individual
Damage to Property (By ATF/TFO)	Selection for video that includes damage to non-ATF property caused by either ATF SA's or TFO's
Damage to ATF Property/Vehicle (by other)	Selection for video that includes damage to ATF property or vehicles by non-ATF employees or TFO's
Litigation	Selection for video that includes FOIA, Bivens, Touhy, torts, media releases

Tag	Description
3 rd Party Individual	3 rd party individual or individuals not associated with the warrant
3 rd Party Vehicle/Tag	3 rd party vehicle or tag not associated with the warrant
Arrest Warrant	Contains execution of a pre-planned arrest warrant
Complaint (IAD, OPRSO)	Video that has been identified as relevant in a complaint against the ATF or an ATF employee
Evidence Seized (By ATF/TFO)	Includes evidence seized by ATF employees or TFO's
Exigent Review Request	DOJ policy exigent review applies
Investigation (IAD)	Identified as relevant in an internal investigation
Litigation-ATF Legal Counsel	Identified as relevant in litigation
Minor Individual	Includes a minor individual
OPRSO	Relevant to OPRSO
Search Warrant	Contains the execution of a pre-planned search warrant
Sensitive Investigative Techniques	Includes sensitive investigative techniques (TOB, EUP, SRT)
Source of Information, CS or UC	Includes a source of information, confidential source or under cover individual
Training (SOD)	Training exercise
ATF Vehicle/Tag	Includes an ATF vehicle or tag
Vehicle Involved Arrest	Includes a vehicle involved arrest
FFL Investigation	Includes evidence involving investigation of a Federal Firearms Licensee
Arson Investigation	Investigation of a suspected Arson
Tag	Description
Explosives Investigation	Evidence involved in an explosives investigation
TBD	
TBD	
TBD	
TBD	
TBD	
TBD	
TBD	
TBD	
TBD	
TBD	

TBD	
TBD	
TBD	
TBD	
TBD	
TBD	

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

(b) (5)

