DEPARTMENT OF HOMELAND SECURITY

U.S. Customs and Border Protection

Request for Information

Body-Worn Cameras in Support of Incident-Driven Video Recording System

Synopsis: This is a request for information (RFI) only. This is an RFI released pursuant to FAR 15.201(e). This RFI is solely for information, planning purposes, and market research only; it does not constitute a Request for Proposal (RFP), Request for Quotation (RFQ), or a promise to issue an RFP or RFQ. This RFI does not commit the Government to contract for any supply or service. U.S. Customs and Border Protection (CBP) will not pay for any costs associated with responding to this RFI. All costs will be solely at the interested party's expense. Not responding to this RFI does not preclude participation in any future RFP or RFQ. If CBP releases a solicitation, it will be posted on the Federal Business Opportunities website (FedBizOpps). CBP advises interested parties to monitor this website for any information that may pertain to this RFI. The information provided in this RFI is subject to change and is not binding on the Government. All responses become the property of the Federal Government upon submission and will not be returned to vendors.

Purpose: This RFI seeks to obtain information and/or recommendations for body-worn cameras (BWC), software for video management and redaction, and cloud storage supporting an Incident-Driven Video Recording System (IDVRS) at CBP. The offerings should meet a desired minimum threshold requested by CBP to meet operational requirements.

Background: CBP is one of the major components of the Department of Homeland Security (DHS) charged with protecting America's borders from terrorism, human and drug smuggling, illegal migration, and agricultural pests while simultaneously facilitating the flow of legitimate travel and trade. As the nation's single, unified border agency, CBP represents the first line of defense of America's borders. CBP agents frequently interact with the public in a variety of operational environments. CBP is interested in potentially using IDVRS at U.S. Border Patrol (USBP).

USBP's mission is to enforce immigration laws and to detect, interdict and apprehend those who attempt to illegally enter or smuggle people or contraband across U.S. borders between official ports of entry. At USBP checkpoints, agents conduct traffic checks to 1) detect and apprehend illegal aliens attempting to travel further into the interior of the United States after evading detection at the border and 2) detect illegal narcotics. USBP checkpoints and stations are often located in remote, unpopulated areas that lack telecommunications or other basic IT infrastructure.

CBP is considering a targeted deployment to expand its audio and video recording capability to record agent interactions with the public using IDVRS. IDVRS includes the use of body-worn cameras (BWC), video management systems (VMS), IT infrastructure, data storage systems, and other interrelated systems supporting incident-driven recordings. CBP is interested in vendors' capabilities to provide three key components of an IDVRS program in tandem: BWC, VMS, and

cloud storage. CBP anticipates storing most footage in CBP-owned data servers, but is also interested in cloud storage for evidentiary footage requiring long-term retention (defined as longer than two years). Footage stored will be secure, law enforcement sensitive data and should comply with all relevant federal laws, regulations, and requirements. CBP also anticipates its users will require a cloud storage platform for frequently accessed files.

CBP is considering a targeted deployment of IDVRS to select known interdiction points where fixed camera systems do not record agent interactions with the public. CBP will prioritize locations based on operational need. This RFI will help CBP to refine its requirements for deploying IDVRS at known interdiction points. Anticipated applications of IDVRS include, but are not limited to, USBP Checkpoint Operations.

Descriptions of these operational environments are included above for further reference.

Capabilities: Table 1 shows the critical operational features, attributes, and minimum thresholds CBP is seeking in an IDVRS capability.

Note: the capabilities listed in this RFI do not constitute finalized requirements and may be adjusted prior to a potential future RFQ or RFP. Vendors should not consider listed capabilities as final or representative of CBP's ultimate requirements.

Table 1: Critical Operational Features, Attributes, Descriptions, and Minimum Thresholds

Critical Operational Features	Attributes	Attribute Description	Minimum Threshold Desired
Information Security	Compliance with federal government security policies	All hardware, software, and services must be compliant with NIST SP 800-53, DHS 4300A Sensitive Systems Handbook, DHS Management Directive 140-01, Information Security Program, and CBP Handbook 1400-05.	Compliance with DHS 4300A "moderate" level of impact.
	Homeland Security Presidential Directive (HSPD) 12 compliance	Security for all vendor applications should be controlled by active directory security grouping. Personal Identification Verification (PIV) credentials should be used for access for federal employees and contractors.	Single sign-on (SSO) using PIV credentials for all vendor applications.
	Federal Risk and Authorization Management Program (FedRAMP)	CBP and DHS require that all cloud products and services meet the standardized approach under FedRAMP	FedRAMP moderate certification for cloud storage platform.
	Video playback	Video playback must be possible using specialized, secure video management software.	N/A
	External drive access	The camera must not allow users to save or download videos directly from the camera to a USB or other external drive/device.	No external drive access.
	Encryption	Video/audio must be encrypted – both data-at-rest and in motion.	Encryption for all data states (at-rest and in motion).

Critical Operational Features	Attributes	Attribute Description	Minimum Threshold Desired
		All components of camera hardware and software must be FIPS 140-2 validated. Systems requiring encryption shall comply with FIPS 197 (Advanced Encryption Standard (AES)) 256 algorithm and cryptographic modules that have been validated under FIPS 140-2.[1] Systems requiring encryption shall comply with National Security Agency (NSA) Type 2 or Type 1 encryption.	FIPS 140-2 Level 4 validation. Compliance with FIPS 197 (AES 256) algorithm, NSA Type 2 or Type 1 encryption.
	User roles/tiered access	Video management software (VMS) must allow administrators to define user roles providing different levels of access (e.g., permission to view videos uploaded by users, permission to redact video, etc.).	Tiered access for different levels of permission in system.
	Domestic data storage	All data must be stored in the continental United States.	Data maintained only in in the continental United States.
	Security operations	Vendor security operations must include: • Design, configuration, implementation, maintenance, and operation of all firewalls within DHS architecture; • Design, configuration, implementation, and maintenance of sensors and hardware required to support the Network Intrusion Detection System (NIDS);	24/7/365 security operations including firewall management, intrusion detection, anti-malware, and patch management services.

[1] Only cryptographic modules that are FIPS 197 (AES 256) compliant and have received FIPS 140-2 validation at the level appropriate to their intended use may be used in systems requiring encryption.

Critical Operational Features	Attributes	Attribute Description	Minimum Threshold Desired
		• Design, implementation, monitoring, and management of a comprehensive anti-malware service; and, • Patch management services. CBP personnel should be able to manage firmware upgrades prior to any patch releases.	
Camera Unit	Singular unit	All camera components should be contained in one unit (no wires extending from camera unit).	Wireless camera unit with no external wiring.
	Storage management	Camera allows agents to continuously record footage without having to manually delete videos to free up storage capacity.	Camera memory equivalent to 12 hours' worth of recorded footage.
	Battery life	Camera should have a battery life such that, if constantly recording, unit will retain power for full life of agent shift.	12-hour battery life if constantly recording.
	Durability	Camera should be water resistant and be able to withstand exposure to saltwater, sun, and other CBP environmental conditions.	N/A
	Secure chain of custody	Agents must not have the ability to edit, modify, or delete recorded data on the camera unit.	N/A
Start/Stop Recording	Agent incident-driven discretion	Users should be able to activate and de-activate the camera manually.	Tactile button to turn camera on/off.
	Pre-event recording	Camera records footage at all times (even when not activated), overwriting and destroying unused footage continuously until activation After activation, camera preserves buffered footage from a set amount of time prior to activation	30 second pre-recording prior to activation. Destruction of footage not actively recorded by officer/agent.

Critical Operational Features	Attributes	Attribute Description	Minimum Threshold Desired
Mounting	Secure	Camera can be securely mounted to agents' uniform, body armor carrier, or duty belt. Camera is able to resist dislodging during movement (especially foot pursuits).	Mount keeps camera secure at all times.
	Upright	The mounting should prevent cameras from rotating or falling off when attached to a uniform, body armor carrier, or duty belt.	Mount keeps camera upright at all times.
Video Offloading	Limited user effort	Camera should possess connectivity to a powered docking station that automatically uploads and downloads to CBP storage infrastructure with limited user effort.	Footage automatically uploads when connected to docking station.
Video Resolution	Clarity	Camera should possess the ability to record high definition quality video.	720p high definition video for recordings.
Audio	Clarity	Camera should record audio with a degree of resistance to wind noise or other ambient noise distortion.	N/A
Data Management	Tagging	Agent should be able to use video management software to categorize video files.	N/A
	In-field tagging	Camera should offer agent option to manually assign tags to videos in the field.	N/A
	Searching	VMS should allow users to search for recorded data based on any manually assigned tag, the date, time, location, weather, Agent's ID/name, or any other camera metadata, including notes written by the agent (i.e., wildcard search).	Wildcard search; search filters corresponding to each manually assigned tag.
	Redaction	VMS should allow authorized users to redact (remove or obscure) personally identifiable information or other sensitive video and/or audio content.	Redaction within VMS without requiring export to additional software.

Critical Operational Features	Attributes	Attribute Description	Minimum Threshold Desired
	Audit trail	VMS should record all user activity, to include any time a user views a video or makes any modifications to video metadata. Log files should be retained for all infrastructure devices, physical access, and anti-malware.	VMS audit log files retained indefinitely. Other log files retained online for 180 days and offline for three years.
	Software management by CBP personnel	CBP personnel must be able to install and manage all software for video management and redaction on secure CBP networks and systems.	N/A
	Scalability	VMS should be scalable and have the ability to manage increased use and volume of audio/video recordings as required by CBP.	N/A
	Metered file transfer	VMS must have ability to send data from local storage to cloud storage at user-specified time(s) of day or night, allowing for off-peak transfer of evidentiary files.	Scheduled data transfer to preserve bandwidth.
	Optimization	VMS provides a certificate and meets other requirements for optimization.[2]	N/A
	Retention	VMS should allow users to set retention periods for footage based on user-assigned tags.	N/A
	New technology	VMS should be able to update and adapt to new file formats, new operating systems, etc.	Update as new technology is released.
Cloud Storage	Cloud storage platform	VMS should connect to cloud storage system to retain evidentiary files for long-term storage.	Connection to long-term storage systems.

[2] Note: CBP currently uses Riverbed network optimization software.

Critical Operational Features	Attributes	Attribute Description	Minimum Threshold Desired
	Ownership of CBP data	Preserve the government's ownership rights over all audio/video data captured using BWC, regardless of vendor ownership of cloud storage platform.	Government ownership of data housed on third-party systems.
	Access to cloud data	Cloud storage platform should allow users to securely share footage.	Recipients can view without installing video management software.
	Interconnection	Interconnections between DHS and non-DHS systems shall be established only through the Trusted Internet Connection (TIC) and by approved service providers.	Use of TIC and approved services providers.
Support	24/7/365 help desk	Technical assistance provided for BWCs and associated hardware, video management software, and cloud storage platform at all times, day or night to service CBP personnel operating around the clock.	24/7/365 hardware and software support.
	Security Operations Center (SOC)	Vendor shall operate a SOC to provide security services related analysis for incidents and incident tracking.	24/7/365 security services. Located in the continental United States.
	Incident response	Vendor shall provide Computer Incident Response Team (CRIT) services.	N/A
	Vulnerability assessments	Vendor shall assist and perform periodic assessments of networks, operating systems, and applications to identify vulnerabilities, and propose mitigations.	N/A
	Training	All users of camera and VMSs receive training offerings prior to using.	N/A
	Clearance	Vendor personnel with video management system access will be required to pass a CBP background investigation.	Public trust clearance for staff supporting IDVRS.

RFI Submission Requirements

Submissions to this RFI are due to the government on Wednesday, October 31, 2019 at 12 noon, Eastern Time. Please send submissions by email to: IDVRS@cbp.dhs.gov, with the email subject line: "(Vendor Name) IDVRS RFI Response." Responses should be in Microsoft Word document file format, including only the response form (pgs. 10-22 of this document). The Government will review all RFI submissions upon receipt and will seek further clarification from respondents, if necessary.

The Government will not publicly disclose vendor proprietary information obtained during this effort. Consistent with the Government's legal obligations, CBP will safeguard information identified by a respondent as "Proprietary or Confidential" to the fullest extent possible. Any information submitted by interested parties in response to this RFI may be shared by the Government with support contractors hired to assist the Government. This includes information marked as limited rights data, restricted computer software, subject to limited rights, or subject to restricted rights. The Government's support contractors that have been, or that will be hired, are required to sign non-disclosure agreements restricting them from unauthorized use and disclosure of information that may be proprietary to third party companies. By submitting information in response to this RFI, respondents are agreeing to allow the Government to share the information they submit with the Government's support contractors who are, or will be, covered by a non-disclosure agreement.

Response Form to Request for Information

Table 2: Company Profile

Company Profile		
Company Name		
Company Address		
Company Website		
Primary Point of Contact	Name:	
	Address:	
	Email:	
	Phone:	
Secondary Point of Contact	Name:	
	Address:	
	Email:	
	Phone:	
DUNS#		
Socioeconomic Status (Check all that apply)	☐Small Business ☐Small Business Disadvantaged ☐8(a) Business ☐Hubzone Business ☐Service-Disabled Veteran-Owned Small Business ☐Veteran-Owned Small Business ☐Women-Owned Small Business ☐Large Business	
Management Systems Capabilities	☐CMMI Level 3 ☐ISO ☐Others – Click here to enter text. (please limit to 500 characters)	
Supplemental Materials	**Please check the box below if you offer supplemental materials indicating capabilities you believe will assist CBP in fulfilling the mission that were not discussed in Table 1 of the RFI**. Please provide any supplemental materials following Table 5 at the end of this response.	

	Please note that supplemental materials provided become the property of the Federal Government upon submission and will not be returned to vendors. Providing supplemental information, while assisting CBP, does not necessarily indicate a better response nor does it guarantee selection in the event CBP issues an RFQ subsequent to this RFI. ☐ We <u>have</u> attached supplemental information regarding our capabilities to the end of the response to this RFI.

Table 3: Capabilities Statement and Description of Products

Capabilities Statement
Please describe corporate experience working with BWCs, VMS, and cloud storage systems.
Different Capability Deliveries
Please check off the types of services that your company can provide in fulfillment of IDVRS. Checking these boxes does not necessarily indicate that your company meets all of the technical specifications, nor does meeting all technical specifications guarantee selection in the event CBP issues an RFQ subsequent to this RFI. Select all that apply.
☐Body-Worn Cameras ☐Video Management System ☐Cloud Storage System
Description of Product(s) Available
Please provide technical literature describing camera capabilities and any available accessories (i.e. part number, video format, recording time, battery life, estimated useful life, warranty terms, end-user training services). Please also include any technical data and/or marketing literature attachments with your response.

Table 4: Claimed Capability Narrative

Critical Operational Features	Attributes	Claimed Capability Narrative Describe specific capabilities related to each desired attribute. Please refer to Table 1 for specific descriptions and minimum thresholds desired by CBP in guiding claimed capabilities.
Information Security	Compliance with federal government security policies	
	Homeland Security Presidential Directive (HSPD) 12 compliance	
	Federal Risk and Authorization Management Program (FedRAMP)	
	Video playback	
	External drive access	
	Encryption	
	User roles/tiered access	

Critical Operational Features	**Attributes**	**Claimed Capability Narrative** Describe specific capabilities related to each desired attribute. Please refer to Table 1 for specific descriptions and minimum thresholds desired by CBP in guiding claimed capabilities.
	Domestic data storage	
	Security operations	
Camera Unit	Singular unit	
	Storage management	
	Battery life	
	Durability	
	Secure chain of custody	
Start/Stop Recording	Agent incident-driven discretion	

Critical Operational Features	**Attributes**	**Claimed Capability Narrative** Describe specific capabilities related to each desired attribute. Please refer to Table 1 for specific descriptions and minimum thresholds desired by CBP in guiding claimed capabilities.
	Pre-event recording	
Mounting	Secure	
	Upright	
Video Offloading	Limited user effort	
Video Resolution	Clarity	
Audio	Clarity	
Data Management	Tagging	
	In-field tagging	

Critical Operational Features	**Attributes**	**Claimed Capability Narrative** Describe specific capabilities related to each desired attribute. Please refer to Table 1 for specific descriptions and minimum thresholds desired by CBP in guiding claimed capabilities.
	Searching	
	Redaction	
	Audit trail	
	Software management by CBP personnel	
	Scalability	
	Metered file transfer	
	Optimization	
	Retention	

Critical Operational Features	**Attributes**	**Claimed Capability Narrative** Describe specific capabilities related to each desired attribute. Please refer to Table 1 for specific descriptions and minimum thresholds desired by CBP in guiding claimed capabilities.
	New technology	
Cloud Storage	Cloud storage platform	
	Ownership of CBP data	
	Access to cloud data	
	Interconnection	
Support	24/7/365 help desk	
	Security Operations Center (SOC)	
	Incident response	

Critical Operational Features	**Attributes**	**Claimed Capability Narrative** Describe specific capabilities related to each desired attribute. Please refer to Table 1 for specific descriptions and minimum thresholds desired by CBP in guiding claimed capabilities.
	Vulnerability assessments	
	Training	
	Clearance	

In addition to the critical operational features listed above, CBP is also interested in learning more about several other features that are of potential interest (see Table 5). As such, CBP is requesting information on these features and the status of implementation. Is this capability currently available? If currently under development, when will it be operational? If applicable, explain why the vendor has decided not to offer the feature at this time.

There is no minimum desired threshold for the features listed in Table 5 as these are topics of interest and not required for IDVRS implementation.

Table 5: Features of Potential Interest

Features of Potential Interest	Attributes of Potential Interest	Attribute Description	Status
Biometric Identify Verification	Facial recognition	Ability to run facial recognition against a database of preexisting images	
	Facial comparison	Ability to compare a source document (e.g., identification provided) against the real-time image of the person	

Table 6: Pricing

Please describe your pricing structure for each of the following items. *Describe whether the items listed below are offered for purchase, lease and/or subscription. Provide cost per unit and any other relevant pricing information.*
Camera
Video Management System
Cloud Storage System
Miscellaneous Costs (e.g., redaction software)

Table 7: Maintenance, Warranty, and Contract Vehicles

Please describe your maintenance concept.
Please provide details of warranty.
Contract vehicles that would be available or recommended to the Government for the procurement of the product.
To include General Service Administration (GSA), GSA Federal Supply Schedules (FSS), or any other Government Agency contract vehicle. This information is for market research only and does not preclude your company from responding to this notice.

Table 8: Questions or Points of Clarification

Please list any questions or points of clarification desired regarding this RFI.