PAMBANSANG PUNONGHIMPILAN TANOD BAYBAYIN NG PILIPINAS
(National Headquarters Philippine Coast Guard)
139 25th Street, Port Area
Manila 1018

NHQ-PCG/CG-11

29 May 2023

STANDING OPERATING PROCEDURES
NUMBER 10-23

UTILIZATION, OPERATION AND MAINTENANCE OF THE PERSONNEL SURVEILLANCE AND VIDEO RECORDING SYSTEM (BODY-WORN CAMERA)

I. AUTHORITY

Republic Act No. 9993, also known as the "Philippine Coast Guard Law of 2009", and its Implementing Rules and Regulations

II. REFERENCES

a. Republic Act No. 10173, also known as the "Data Privacy Act of 2012", and its Implementing Rules and Regulations

b. Republic Act No. 9995, also known as "Anti-Photo and Video Voyeurism Act of 2009", and its Implementing Rules and Regulations

c. Administrative Matter No. 21-06-08-SC, "Rules on the Use of Body-Worn Cameras in the Execution of Warrants" dated 29 June 2021

d. HPCG/CG-8 SOP Nr 09-12, "Pre-Departure Inspection of Vessel"

e. HPCG/CG-8 Memorandum Circular Nr. 07-12, "Pre-Departure Inspection"

f. CPCG Memorandum dated 26 June 2012, "Guidelines on Video Recording during Mandatory Pre-Departure Inspection"

III. PURPOSE

This prescribes the policies and procedures on the effective and legal use of Personnel Surveillance and Video Recording System (Body-Worn Camera) to strengthen law enforcement capabilities of PCG such as maritime security and other law enforcement operations in the form of capturing photos and recordings during maritime operations with its capability of real-time video streaming, play back and remote access. Also, for reviewing operations conducted, for planning future operations, and pursuing legal remedies such as filing and evidence collection.

IV. SCOPE

This applies to the use of Body-Worn Camera issued to concerned PCG Units and Personnel carried while performing PCG duties, particularly in the conduct of law enforcement operations.

This SOP covers proper turnover of equipment from one unit / personnel to another, proper utilization of equipment during operations, proper turnover of stored data, captured photographs or videos from one unit, personnel, or system to another, and proper maintenance of equipment.

V. DEFINITION OF TERMS

For the purpose of this SOP, the terms below are defined as follows:

a. **Body-Worn Camera (BWC)** – refers to an electronic camera device for generating, sending, receiving, displaying and processing audio-visual recordings that may be worn during PCG law enforcement activities from the site of operation, and can be viewed from the Regional Center and Command Center;

b. **BWC Operator** - refers to any PCG personnel authorized to carry the BWC and who has been issued with an RFID Card;

c. **Coast Guard Information System (CGIS)** – refers to a major sub-unit of CGWCEISC that specializes in information systems;

d. **Coast Guard Maritime Communications and Electronics (COMELS)** – refers to a major sub-unit of CGWCEISC that specializes in maritime communications and electronics system;

e. **Command Center (CC)** – refers to Headquarters Coast Guard Weapons, Communications, Electronics and Information System Command (HCGWCEISC) Mandaluyong and/or NHQ-PCG as the center of PCG's Information System capable of storing large amounts of recorded videos, audios, photos, data and capable of remote live streaming from all RCs up to an estimate of 100 BWC simultaneously;

f. **Communication Electronics (COMMELEX)** – refers to the specialized field concerned with the use of electronic devices and systems for the acquisition or acceptance, processing, storage, display, analysis, protection, disposition and transfer of information;

g. **Dock Controller –** refers to a device that has a Gigabit Ethernet output port for network connectivity and which connects directly to the docking trays for the BWC and to the VSS; serves as temporary storage of data when the VSS is offline or not connected to the Dock Controller;

h. **Docking Station** – refers to a hub, port and terminal with an 8-slot docks connected to a Dock Controller unit suitable for connecting, uploading video and rapidly charging up to eight (8) BWC units simultaneously;

i. **Data SIM** – refers to a subscriber's identity module card installed to all BWC units with data connectivity that enables live streaming even over 2G/3G/4G at bandwidths as low as 9 Kbps;

j. **Evidence Management System (EMS) –** refers to an encrypted system that is used to receive, store, track and manage evidence in the form of photographs or videos that are capable of viewing or monitoring using a device such as in workstation, desktop, laptop, tablet and smartphone;

k. **Radio Frequency Identification Reader (RFID Reader)** – refers to a device with detection feature and capability so that it will easily recognize the BWC user. The BWC can be quickly assigned to an operator when they present their RFID ID card to the reader. The RFID card reader is directly connected to the Dock Controller;

l. **CGWCEIS Regional Center (RC)** – refers to the Operational Control Units of CGWCEISC assigned in Coast Guard Districts and put in charge of the system operation and management including the preventive maintenance of the equipment (such as Laptop, Tablet, BWC Unit, Docking Station, Dock Controller and RFID Reader) in their respective districts or area of responsibilities;

m. **System Administrator** – refers to an authorized CGIS Personnel who can only access the Evidence Management System (EMS) and RFID Registration System; Responsible for the data storing, retaining and monitoring;

n. **Team Leader/Officer-in-Charge** – refers to Coast Guard District or Major Unit personnel responsible for the conduct of operation where BWC shall be used;

o. **Video System Server (VSS)** – refers to a managed file for up to 100 cameras. The exact number of cameras supported depends on how much video file is being collected each day and how long it is kept for.

VI. POLICIES

a) All Coast Guard Districts shall have CGWCEIS RCs with BWC, VSS, EMS and RFID support and capabilities, including Dock Controller and Dock Stations.

b) VSS and EMS should provide secured platforms and data stored therein should be encrypted and replicated in HCGWCEISC CC.

c) All CGWCEIS RCs should have reasonable number of BWCs and related equipment.

d) All CGWCEIS RCs should have at least one System Administrator.

e) Only the designated System Administrators are allowed to access the RFID Card Registration System and the EMS.

f) No PCG personnel shall be designated as BWC Operator without undergoing the complete BWC training/familiarization.

g) District Commander shall identify the BWC Operators and issue RFID Cards with the corresponding Inventory Custodian Slip (ICS).

h) RFID Cards are non-transferable upon issuance. In case the BWC Operator is reassigned, relieved, undergoing training / schooling, on leave / rest and recreation, discharged, suspended or separated from the service, the RFID Card can be reassigned to another BWC Operator, following the prescribed procedures concerning the transfer of accountability.

i) BWC Operator shall be the primary responsible for the RFID Card and BWC issued to him/her. Any loss or damage to the RFID Card and/or BWC due to his/her negligence, as determined after the conduct of proper investigation shall be on the account of the concerned BWC Operator.

j) CGWCEIS RCs should only issue BWCs and a laptop or tablet to Response Team/BWC Operators upon presentation of a mission order or with the direct instruction from the District Commander; issuance shall be with a BWC Deployment Form (Annex "A").

k) Only authorized software application is allowed to be installed on the issued tablet, laptop and/or desktop. Any unauthorized application installation/usage of the equipment will be reported immediately to HCGWCEISC for appropriate disciplinary action.

l) All BWCs and related equipment are for use solely in the course of official duties/activities and shall not be used for personal purposes. Non-PCG Personnel are prohibited from using the issued BWCs.

m) Intentionally turning off the BWC to prevent recording of any incident likely to hold the BWC Operator liable is prohibited and is subject to investigation.

n) CGWCEIS RCs, particularly the System Administrator, shall ensure that the images/audio-visual footages as captured/recorded by the BWC devices are uploaded to the VSS.

o) Images and footages captured by BWC shall not be disclosed unless sanctioned by competent authorities.

VII. PROCEDURE

a. Training

1. Prior to the installation or setting up of the BWC System which includes the VSS, EMS and RFID System, the prospective System Administrators, CGIS and COMMELEX Personnel must complete the pertinent trainings on the operations, principles and management of the BWC System.

2. Similarly, prospective BWC Operators must be identified and sent for the pertinent training concerning the operation of BWC.

b. Operation

1. **Signing Out of BWCs and Issuance of its Accessory Equipment**

a) For ad hoc or special operations, Unit Commander shall recommend a list of the BWC Operators to be issued with RFID Cards for the approval of the District Commander. CGWCEIS RC shall issue the RFID Cards to BWC Operators based on the approved list with the corresponding ICS in accordance with the "Guidelines for Video Recording during Mandatory Pre-Departure Inspection".

b) Upon receipt of a Mission Order/Directive to perform an operation/mission, the Team Leader/OIC of said Unit shall request from CGWCEIS RC for the issuance of BWCs, laptops and/or tablets, and additional RFID Cards in exceptional or special cases.

c) Upon receipt of the request, CGWCEIS RC shall conduct an equipment check on BWCs, laptops and/or tablets before issuing the equipment to ensure good condition and to identify/note any damage or malfunctions prior to use.

d) Once CGWCEIS RC is done with the equipment check, it shall inform the Response Team to receive the equipment. The Team Leader/OIC shall secure a BWC Deployment Form (Annex "A").

e) In selecting the BWCs, the BWC Operator must tap their RFID Cards to the RFID Reader; the system will analyze the available BWCs and will pulse a light on BWC that is fully charged and allocate the same to the BWC Operator. Aside from electronically signing out the BWC thru RFID, the CGWCEIS RC shall ensure that the same is logged in the logbook. Also, the Team Leader/OIC shall reflect the same in the BWC Deployment Form.

2. **Utilization of BWC**

a) Prior the conduct of an activity/operation/ mission/deployment, the Unit Operations (Districts/Stations) shall inform the HCGWCEISC CC and PCGCC to establish remote monitoring especially in the event of high risk, sensitive and critical activity/operation/mission/deployment.

b) During deployment, BWC shall be worn preferably on the shoulder or central body, provided that it is safely secured with a harness or other available accessories and will capture a good view. However, if long firearms are used, BWC must be attached to the operator's tactical helmet, provided that it is available.

c) BWC Operators shall turn "ON" the device (Annex "C") and ensure that Active Mode is enabled before the start of operation and the BWC shall not be deactivated until the operation has been fully concluded and the personnel conducting the operation have left the premises and returned to the proper station.

d) BWC Operators shall press the record button (Annex "C") to go to "pre-record" mode. The "pre-record" mode stores at least thirty (30) seconds of footage or depends on the configuration prior to record activation, operating as a constant buffer.

e) Once the camera is activated in recording/live streaming mode, it shall remain "ON" until the activity is completed or it runs out of battery. In case the BWC has low battery status, a universal cellphone charger can be used as an alternative charger in the area.

f) Whenever the BWC Operator feels threatened/uncomfortable concerning his/her safety and when on live streaming, a "panic button" can be activated (Annex "C") to notify the CGWCEIS RC and CC about the presence of a threat by pressing the "panic button" 1-2 times or as needed.

g) During deployment/mission, any functionality or serviceability problem shall be immediately reported directly to the Team Leader/OIC and arrange for a replacement device if possible. Said incident should be included in the after-deployment report.

3. **Uploading of Files**

a) Upon return from deployment/mission, the Team Leader shall instruct BWC Operators who are part of the deployment/mission to bring their BWCs to RC for signing in and uploading of files.

b) System Administrator shall place the BWC in a Docking Station that is connected to the Dock Controller to upload the files. BWC should not be removed from the Docking Station until all of the data has been uploaded/transferred. When the Dock Controller is connected to the internet, the data will be stored directly to VSS where it can be viewed remotely using the EMS.

c) Once uploading is done, the storage of BWC shall be automatically cleared out for the next deployment. The System Administrator may let the BWC in the Docking Station for it to be recharged.

4. **Signing In of BWCs and Return of Other Equipment**

a) At the end of deployment/mission, prior to or after uploading the files from BWC to VSS, the BWC Operators, in the presence of the System Administrator, shall place their respective BWCs on the Docking Station and tap their RFID Card on the RFID Reader to sign in the BWC.

b) Likewise, laptops and/or tablets shall be returned to System Administrator. Both the System Administrator and Team Leader/BWC Operator shall inspect for possible damages on the returned equipment. Also, the System Administrator shall indicate his/her remarks in the BWC Deployment Form to be signed by him/her and by the Team Leader and/or BWC Operators.

c) The System Administrator shall log in the logbook the signing in of BWCs and the return of other equipment, including the damages noted.

d) The System Administrator or other COMMELEX Personnel shall ensure that the BWCs and other equipment are kept in a secured location when not in use.

5. **Reviewing of Files**

a) System Administrator and Team Leader/OIC shall review the photographs or videos after every deployment or depending on the availability of equipment. The System Administrator and Team Leader/OIC should properly tag the videos uploaded to the VSS.

b) The System Administrator should monitor, using EMS, the images and/or footages uploaded to VSS and shall report to Coast Guard Intelligence Group (CGIG) for any censored images and footages captured by BWC.

c) When investigation warrants, data should be forwarded to CGIG-IAS for personnel investigation, MCI for Safety investigation, and/or CGIDMS for criminal investigation. CGIG shall review the videos in the presence of the System Administrators, Team Leader/OIC and the offender/perpetrators prior writing a report to ensure impartiality and consistency.

6. **Release of Recordings**

a) All data, images, videos and metadata captured, recorded or otherwise produced by the equipment are sole property of the Philippine Coast Guard (PCG), and shall be securely stored and retained in accordance with applicable laws (such as RA No 10173 or the "Data Privacy Act of 2012").

b) Team Leaders/OICs, BWC Operators and other PCG Personnel, both uniformed and civilian employees, shall not edit, alter, erase, duplicate, copy, share or otherwise distribute BWC recording videos without prior written approval. Any reported duplication or distribution of sensitive or confidential videos shall be the full responsibility of the Unit Commander.

c) Requests for copies of data, images or videos by persons or other agencies must be done in writing and addressed to Unit Commander or HCGWCEISC; the requests shall be recommended by HCGWCEISC for the written approval of CPCG.

d) Posting of footage in any social media site without prior written approval from Unit Command or HCGWCEISC is strictly prohibited.

7. **Maintenance**

a) After deployment, any functionality or serviceability problems with the BWC and other equipment during deployment/mission shall be reported to the CGWCEIS RC.

b) The CGWCEIS RC shall perform diagnosis and repair. Any unresolved issues must be properly documented in writing and reported to the District and HCGWCEISC. HCGWCEISC shall request funding requirements from O/CG-11 for the repair and maintenance of equipment.

c) CGWCEIS RC shall ensure proper maintenance of the equipment and system; he/she must submit a monthly maintenance report to Headquarters Districts (Attn: D11) prior to submission to HCGWCEISC and O/CG-11.

VIII. PROHIBITED ACTS

a. Transfer of RFID Cards without following the proper procedures.

b. Installation of unauthorized software on the issued tablet, laptop and desktop dedicated to BWC.

c. Intentionally turning off the BWC to prevent recording of any incident likely to hold the BWC Operator liable.

d. Using BWC for personal purposes.

e. Using BWC other than those issued by PCG.

f. Lending BWC to other agencies.

g. Accessing, copying, altering, distributing and deleting or any form of personal consumption of data, photos and videos without authority or approval from the District/Major Unit Commander.

h. Any violation on the stated prohibitions under this section shall be subject to the applicable penal provisions of RA 10173 and RA 9995 and their respective implementing rules and regulations.

IX. RESPONSIBILITY

a. **DCS for MCWEIS, CG-11**

1. Provide policy, procedural guidance, and coordination of action, including planning, training and proper implementation of this SOP in coordination with CGWCEISC;

2. Ensure funding for the repair, maintenance, monthly data allocation and other operational expenses of all BWCs;

3. Consolidate and evaluate reports prescribed in this SOP;

4. Supervise the implementation of this SOP; and

5. Perform other tasks as may be directed.

b. **Commander, CGWCEISC**

1. Appoint or designate Data Privacy Officer;

2. Ensure that all CGWCEIS RCs have enough COMMELEX and CGIS Personnel specifically trained in the administrative management and proper maintenance of the System;

3. Ensure that CGWCEIS RCs have enough equipment to realize the purposes of this SOP;

4. Provide access or delegate such authority to give access, to all or some BWC-related systems, including mirroring capabilities of mobile phones, tablets and laptops;

5. Approve requests for copies of data, images and videos from concerned persons or other agencies;

6. Through CGWCEIS RCs, CGWCEISC Major Units and/or HCGWCEISC CC, ensure collection of reports from all Districts/Units and consolidation thereof on matters pertaining to BWC;

7. Ensure strict compliance with the provisions of this SOP and initiate appropriate action in case of violations; and

8. Perform other tasks as may be directed.

c. **Commanding Officer, CGWCEIS Regional Center**

1. Assume the duties and functions of the System Administrator or delegate the same to qualified CGWCEISC Personnel;

2. Ensures the security and integrity of data, and report any breach immediately upon knowledge or receipt of a report of such breach;

3. Issue RFID Cards to all designated BWC Operators, and release/issue the BWCs, laptops and/or tablets upon receipt of order/directive or Mission Form;

4. Conduct inspection and maintenance of BWCs at least once a month or as needed and/or upon issuance of BWC or receipt of the same;

5. Manage and maintain all related system such as the VSS, EMS, Dock Controller and Stations, and RFID Registration System, including the hardware, equipment and paraphernalia; ensures that the Software and Encoder Firmware of the System are updated;

6. Ensure that failure diagnosis and all unresolved issues are properly documented in writing and reported to the District and HCGWCEISC (Attn: WCEIS-6); and

7. Keep, maintain and update logbooks or other record books including inventory, maintenance, incident reports and ensure submission of the same to concerned parties such as HCGWCEISC and O/CG-11;

8. Perform other tasks as may be directed.

d. **Commander, Coast Guard Districts/Major Commands**

1. Approve the list of authorized BWC Operators or personnel to be issued with RFID Cards, as recommended by the Operations Officer;

2. Approve the issuance of mission order, including the directive for the use of BWC;

3. Approve and/or recommend or endorse to National Headquarters, all requests for copies of data, images or videos by concerned persons or other agencies; and

4. Ensure that the provisions of this SOP are strictly followed and to initiate investigation, submission of reports etc., and to take appropriate actions in case of violations;

5. Perform other tasks as may be directed.

e. **Unit Operations Officer (D3)**

1. Identify and recommend to Commander, Coast Guard District/Major Command such Personnel who shall be issued with RFID Cards; ensure that issuance thereof is evidenced by PAR/ICS;

2. Release/issue Order/Directive for the issuance of BWC;

3. Render reports for any lost or damage on the BWC, and submit to Headquarters Districts (Attn: D11) prior submission to HCGWCEISC and O/CG-11;

4. Ensure that the D-11 and HCGWCEISC CC and PCGCC are informed on the deployment of BWC to establish remote monitoring especially in the event of high risk, sensitive, critical and important activity/mission/deployment; and

5. Perform other tasks as directed.

f. **Team Leader/Officer-in-Charge**

1. Before the conduct of operation, identify and recommend Personnel, only those with issued RFID Cards, to be designated as BWC Operators for that particular mission or operation;

2. Accomplish the necessary BWC Deployment Form (*Annex "A"*) prior to deployment and state therein any untoward incident that occurred during the conduct of operation;

3. Take charge during the on-set of operation; supervise the BWC operator on proper utilization and operation of BWC; monitor personnel for any unlawful copying, transfer, sharing or altering of data;

4. Ensure that BWC and the laptops and/or tablets are returned, and ensure or direct BWC Operators to ensure that the data contained in the BWCs are uploaded to VSS;

5. Perform other tasks as may be directed.

g. **Body Worn Camera Operator**

1. Take good care of the RFID Card issued to him/her;

2. Ensure that the BWC signed out is working properly upon receipt and before deployment;

3. Handle and use BWC properly and responsibly;

4. Observe strict compliance with the provisions of this SOP concerning the usage of equipment and the integrity and confidentiality of data;

5. Report any malfunction of the equipment or any untoward incident during deployment/operation;

6. Perform other tasks as may be directed.

X. RESCISSION

All PCG issuances and other publications inconsistent with this SOP are hereby repealed, amended or modified accordingly.

XI. EFFECTIVITY

This SOP takes effect upon publication.

BY COMMAND OF COAST GUARD VICE ADMIRAL PUNZALAN JR:

OFFICIAL:

TITO ALVIN G ANDAL
CG COMMO
Chief of Coast Guard Staff

JAYSIEBELL B FERRER
CG CDR
Coast Guard Adjutant

Annexes:

A – BWC Deployment Form
B – Guidelines for Video Recording during Mandatory Pre-Delivery Inspection
C – BWC Picture Diagram
D – Support Ticket Form

ANNEX A

DEPLOYMENT FORM

PERSONNEL SURVEILLANCE AND VIDEO RECORDING SYSTEM (BODY WORN CAMERA)

O/D3

D.FORM CONTROL NR: _____

DATE: _____

PURPOSE: _____

_____

	OPERATOR/S	ITEM/DESRIPTION	CODE NR
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			

Deployment Report:

(use separate sheet/s if needed)

Inspection Remarks:

Inspected and Issued by:

_____

System Administrator/WCEIS-RC

Inspected and Received by:

_____

System Administrator/WCEIS-RC

Received by:	Turned-in by:	Authority by:
_____	_____	_____
Team Leader/OIC	Team Leader/OIC	D3/Duty CDO

Note/s: 1) Use another D.Form with separate control number if there will be more the ten (10) Operators are to be deployed;
2) This form shall be reproduced in two (2) copies (D3 and WCEIS-RC).

TANGGAPAN NG KOMANDANTE
(OFFICE OF THE COMMANDANT)
PUNONGHIMPILAN TANOD BAYBAYIN NG PILIPINAS
(Headquarters Philippine Coast Guard)
139 25th Street, Port Area
1018 Manila

MEMORANDUM

To	:	**ALL COAST GUARD DISTRICTS**
From	:	**COMMANDANT, PHILIPPINE COAST GUARD**
Subject	:	Guidelines for Video Recording during Mandatory Pre - Departure Inspection
Date	:	26 June 2012

1. In compliance with the instruction of Secretary, Department of Transportation and Communications to strengthen the maritime safety enforcement of the PCG through conduct of Mandatory Pre-Departure Inspection (MPDI) of all vessels, the video recording will form part of the MPDI system. Hence, all Coast Guard District Commanders are directed to ensure the inclusion of video recording during the conduct of MPDI at their respective District AOR's.

2. The following are the preferred points for video recording during MPDI:

External Hull	- Hull, Plimsol/ loadline marks and forward and stern draft mark, accommodation/embarkation ladder arrangement, anchor, safety net.
Safe Cargo Handling	- General appearance of cargoes to show if they are properly lashed and how they are lashed and stowed.
Passengers	- Adequate accommodation spaces for passengers and other spaces (restaurants, stores, hall/passage ways and weather deck.
Safe Navigation	- Operational status of navigational equipment, completeness of voyage charts and publication, bridge visibility, running lights.
Communication and Radio Equipment	- Operational status of radio equipment, radio installation and public address system.
Life Saving Appliances	- Lifeboats and securing boats, launching arrangement, life rafts, personal lifesaving appliances.

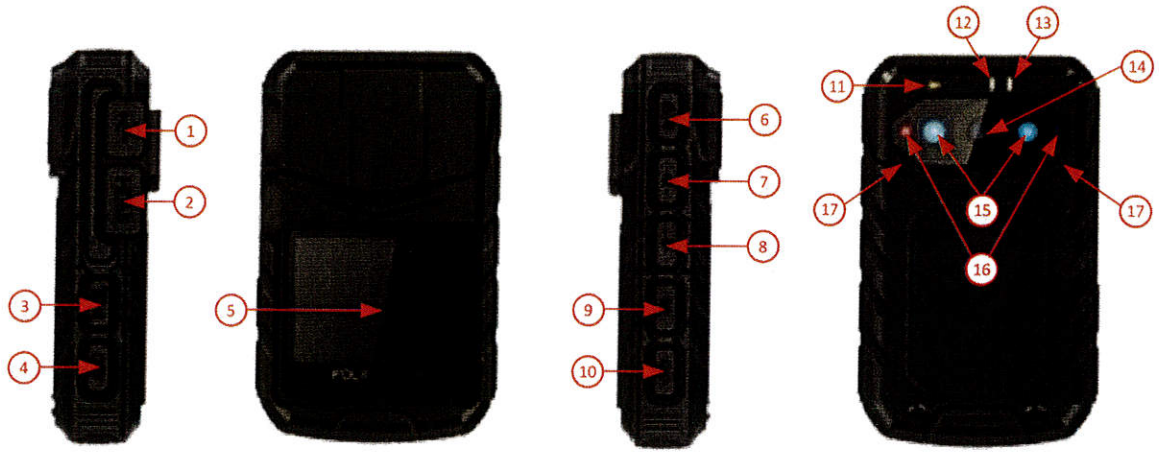
Engine Room	- Main and auxiliary engines, pipings, pumps, valves, cleanliness of machinery spaces, emergency escape route, steering gears, generator.

3. The inclusion of video recording during MPDI is applicable preferably to major ports only subject to the availability of video camera. PCG Districts will maintain a copy of recorded MPDI video respectively and be made available for ready reference of the Command.

4. For guidance and strict compliance.

EDMUND C TAN
VADM PCG

ANNEX C



(LEFT SIDE VIEW) (REAR VIEW) (RIGHT SIDE VIEW) (FRONT VIEW)

Diagram No	Connector / Indicator Purpose	Conn No	Connector / Indicator Purpose
1	USB Connector	10	Power on / off (long press)
2	HDMI (Not Supported)	11	Undock LED
3	Stop / Start Recording	12	Data LED
4	Panic Button	13	Power / Charging LED
5	LCD TFT Screen	14	Camera Lens
6	Facial Recognition (Not Supported)	15	IR Lamps
7	IR Lamps On / Off	16	Ambient Light Detectors
8	Silent Mode (Stop Beeps)	17	Microphone
9	No Function		

***ANNEX D*: Support Ticket Request Form**

CHAPTER 5-2: RAISING A SUPPORT TICKET

CONTENTS:

TABLES:

RAISING A SUPPORT TICKET

Introduction

1 This chapter details the procedure to be taken to obtain third or fourth line support from Digital Barriers; this can be used for the following circumstances:

1.1 To ensure a resolved unexpected issue is reported, so that the relevant support personnel can earmark it for investigation if required.

1.2 To ensure an unresolved issue is reported to gain third line support (regional).

1.3 To ensure an unresolved issue is reported to gain fourth line support (national).

2 Any competent person that has received training on the system can complete this procedure and request a Support Ticket be raised.

Originator Procedure

3 The procedure for raising a support ticket is as follows:

3.1 Identify Fault.

3.2 Complete Support Ticket Request Form on Page 1 (instructions at footnote).

3.3 Attach the form to an E-mail with the Subject Line stating a quick summary of the fault e.g. - ***BW500 will not Record*** - to the following E-mail addresses:

3.3.1 **To**: support@tvisupport.freshdesk.com

3.3.2 **CC**: asiasupport@digitalbarriers.com

Follow-on Action

4 A Support Ticket will automatically be created thus ensuring that the relevant personnel with the DB Support chain are advised and any necessary follow up action will ensue.

5 The originator will be notified by DB Support, within 24 hours, of any action being taken to resolve the issue.

Ticket Closure

6 The Support Ticket originator will be notified by DB Support when the issue / incident has been resolved - they will be given the chance to comment on the process and indicate that they are content for the ticket to be closed.

***ANNEX D*: Support Ticket Request Form**

PCG Unit/System Administrator Reporting Fault (E-mail)	
Subject (Brief Fault Description)[1]	
Region	Asia Pacific
Product Type[2]	
EdgeVis Viewer Version[3]	
EdgeVis Server Version	v7.2.3
Encoder Firmware Version[4]	
Customer Reference Number[5]	
Full Fault Description[6]	

[1] Give a brief one line over view of fault – e.g. *BW500 does not connect to Server.*

[2] E.g. *Q800 Encoder* or *BW500 Camera.*

[3] This can be found under ***About...*** section from Hamburger symbol - top right of home Page of EdgeVis Client.

[4] Can be located under ***Status and Diagnostics*** menu when ***Configure Encoder*** is selected from EdgeVis Client - enter ***Not Known*** if Encoder does not connect to Server!

[5] Enter Unique Number if Fault Database kept by Originator – enter ***Not Applicable*** if none required.

[6] Enter as much detail as possible - this will ensure that DB Support have all the information required to investigate the issue.