

# CAYMAN ISLANDS GOVERNMENT

# National CCTV Programme

# **CODE OF PRACTICE**

Approved by Cabinet
19 July 2011

# NATIONAL CCTV PROGRAMME CODE OF PRACTICE

# **CONTENTS**

- 1. INTRODUCTION
- 2. GENERAL PRINCIPLES and OVERSIGHT
- 3. PARTNERSHIPS WITH PRIVATE SECTOR ENTITIES
- 4. CIVIL LIBERTIES
- 5. DATA PROTECTION
- 6. RESPONSIBILITY FOR THE SYSTEM
- 7. CAMERA POSITIONING, COVERAGE AND SIGNAGE
- 8. CONTROL, MONITORING AND OPERATION OF CAMERAS
- 9. STAFF AND TRAINING
- 10. GENERAL TAPE RECORDED MATERIAL
- 11. EVALUATION
- 12. EVIDENCE
- 13. EVIDENTIAL RECORDED MATERIAL
- 14. IDENTIFICATION PROCEDURES
- 15. MEDIA
- 16. ACCOUNTABILITY AND COMPLAINTS
- 17. ACCESS TO THE ELECTRONIC MONITORING CENTRE
- 18. FREEDOM OF INFORMATION LAW
- 19. APPENDIX A NATIONAL CCTV MASTER CAMERA LIST
- 20. APPENDIX B SAMPLE CCTV SIGNS
- 21. APPENDIX C PRIMARY AND SECONDARY MONITORING LOCATIONS
- 22. APPENDIX D LIST OF AUTHORIZED CCTV OPERATORS
- 23. APPENDIX E CAMERA LOCATIONS MAP

# **CCTV Code of Practice**

Code of practice relating to the use of overt public surveillance Closed Circuit Television (CCTV) systems that are monitored by and directly linked to the Cayman Islands Electronic Monitoring Centre (CIEMC), Cayman Islands Emergency Communications Centre (CIEC911) and the Royal Cayman Islands Police Service (RCIPS) through the auspices of the Portfolio of Internal & External Affairs, (Portfolio), Cayman Islands Government (CIG).

#### 1. INTRODUCTION

- 1.1 In recent years, the Cayman Islands have witnessed a disturbing increase in the number of violent crimes being committed. It is expected that the National CCTV Programme will play a key role in the Territory's national security policy both in terms of deterring the commission of crimes and for capturing vital evidence for use in criminal prosecutions. The National CCTV Programme is led by the Portfolio of Internal and External Affairs in consultation with the National CCTV Programme Committee.
- 1.2 The aims of the National CCTV Programme are to:
  - (i) reduce the fear of crime;
  - (ii) promote community safety;
  - (iii) stimulate continuing economic growth within the community;
  - (iii) encourage the use of public and commercial facilities;
  - (iv) assist in the reduction, prevention and detection of crime;
  - (v) provide high quality evidence to be used by the RCIPS, Immigration, and Customs to prosecute offenders;
  - (vi) monitor road traffic circulation and improve road safety;
  - (vii) protect public property.
- 1.3 At present there is no statutory framework for the regulation of CCTV use, either Government- or privately-operated in the Cayman Islands. In due course, this will be provided through a Data Protection Law. This legislation will regulate the processing and use of images captured by CCTV cameras. It will also establish the usage of an independent oversight body the Office of the Information Commissioner for CCTV matters as it relates to Human Rights concerns. The Office of the Information Commissioner, in addition to approving a National Code of Practice for both public and private CCTV system operators, will investigate complaints and claims of statutory breach or infringement.
- 1.4 Until data protection legislation comes into effect, the National CCTV Programme will be operated in accordance with this Code of Practice. The Code is based on recognized data protection principles and existing best practice standards in the public use of CCTV. It also takes into account civil liberties, especially the fundamental right to privacy as provided for in Article 8 of the European Convention on Human Rights. Whilst the Code does not have the binding effect of legislation (nor does it purport to be an adequate substitute for legislation), it represents a solid platform for ensuring that a proper balance is achieved between the needs of national security and protection of the rights of individuals. The Code also seeks to reassure the public about the safeguards that are in place to protect those rights.
- 1.5 Given that the National CCTV Programme may include the use of some privately operated CCTV systems, it is anticipated that those private sector operators will also adopt the good practices contained in this Code of Practice until data protection legislation comes into force.

#### 2. GENERAL PRINCIPLES and OVERSIGHT

- 2.1 The Cayman Islands Government recognizes that the use of CCTV necessarily involves intrusion into the lives of ordinary individuals as they go about their daily business. In order to maintain public confidence in the National CCTV Programme, it is essential that public video surveillance is handled responsibly with effective safeguards in place to ensure that any interference with the right to privacy is lawful, necessary and proportionate. Such public trust is critical for the benefits of CCTV to be fully realized. With these factors in mind, the Cayman Islands Government commits to the following general principles. These principles are expanded upon in later sections of this Code.
  - (i) The Cayman Islands Government fully supports the use of video surveillance in public areas to achieve the purposes outlined at clause 1.2, subject to there being appropriate local consultation involving the business community, the Human Rights Commission and the public in regards to requirements of future Data Protection Legislation and its interaction with the Bill of Rights which will come into force in November 2012. Consultation with these groups is necessary because the use of public video surveillance must be proportional in its use to meet the stated aims. Periodic consultation will be necessary to carry out an evaluation of what the perceived threats are (and therefore if the stated aims are still relevant) and what the proportionate response to those threats should be.
  - (ii) The Cayman Islands Government will create a National CCTV Programme Advisory Committee, which will include members of the public. The Committee will meet no less than twice a year to review, advice, and provide consultation on the operational aspects of the Programme.
  - (ii) The Cayman Islands Government will set performance criteria for the quality of the recorded images produced by CCTV systems, and will insist that these standards are maintained.
  - (iii) No audio recording facility will be used in conjunction with CCTV cameras.
  - (iv) The following data protection principles will apply to images captured by the National CCTV Programme. The images shall be:
    - fairly and lawfully processed
    - processed for limited purposes
    - adequate, relevant and not excessive
    - accurate and up to date
    - kept no longer than necessary
    - processed in accordance with the individual's rights
    - secure

Data protection principles contained in data protection legislation provide a means of regulatory control of the use of CCTV systems so that individuals may enjoy security of their safety and possessions whilst being assured that rights to

personal privacy will not be unlawfully compromised. Adopting proper standards of practice in line with forthcoming legislation will help towards realizing these objectives.

- (v) Fair and lawful use of CCTV equipment requires that the public must be informed that their images are being captured. This is accomplished by the posting of appropriate signage in areas in which the National CCTV System is deployed. (See chapter 7).
- (vi) CCTV images are to be collected, retained, used and destroyed properly and safely. (See chapters 8-10)
- (vii) In order to protect individual privacy, the equipment should be located and configured in such a way that it only monitors those public spaces which are intended to be covered by the equipment. (See chapter 7).
- (viii) Disclosure and custody of recorded images shall be conducted in strict accordance with proper guidelines. (See chapter 13).
- (ix) CCTV surveillance under the National CCTV Programme is strictly limited to the aims expressed in clause 1.2 and will not be used for entertainment or commercial purposes or indiscriminately.
- (x) A Complaints Procedure shall be available to the public to address privacy concerns relating to alleged non-compliance with the provisions of this Code of Practice or the Procedure Manual.
- 2.2 Overall responsibility for the operation and maintenance of the System will rest with the Emergency Communications Manager of the Cayman Islands Emergency Communications and Electronic Monitoring Centre.
- 2.3 Evaluation of the performance and achievements of the National CCTV Programme will be undertaken at quarterly intervals to ensure that the standards required by this Code are being complied with. This will be undertaken by a committee including representatives from the Portfolio of Internal & External Affairs, the Cayman Islands Emergency Communications and Electronic Monitoring Department and the Royal Cayman Islands Police Service. During evaluation, careful consideration will be given to issues arising in respect to privacy.
- 2.4 Subject to operational requirements and national security issues, factual information on the numbers of cameras and the statistical findings of the evaluation processes should be published periodically and not less frequently than once per annum.

#### 3. PARTNERSHIP WITH PRIVATE SECTOR ENTITITES

3.1 The National CCTV Programme will from time to time include the use of some cameras which are operated and controlled by private sector entities. By way of a Memorandum of Understanding, any private sector entity so involved will commit to upholding the principles and standards contained in this Code. Any failure to honour this commitment may lead to the termination of the company's involvement in the National CCTV Programme. The purpose for which the system is established should be clearly identified. This is particularly important should evidence be required to be drawn from systems independent of the Government. In anticipation of Data Protection legislation, private organizations and/or individuals entering into agreements with the National CCTV Programme would be required to adopt the principles of Data Protection in advance to show a commitment to ultimate compliance with the future Data Protection Law. The purpose of this adoption of Data Protection principles is to strengthen the admissibility of evidence obtained via such private entities.

#### 4. CIVIL LIBERTIES

The Cayman Islands Government is committed to upholding the fundamental right to privacy as provided for by Article 8 of the European Convention on Human Rights and as expressed in Article 9 of Part 1 of the Cayman Islands Constitution Order 2009.

The object of Article 8 (and the corresponding clause in Article 9 of Part 1 of the Constitution) is to protect the individual against arbitrary interference by public authorities. It states as follows:

- "8(1) Everyone has the right to respect for his private and family life, his home and his correspondence.
- (2) There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

It can be seen from Article 8(2) that the right to privacy is a qualified right and that there are occasions when interferences are justified. But this involves careful consideration of a number of factors:

- Is the proposed system established on a proper legal basis and operated in accordance with the law?
- Is the interference necessary to address a pressing need, such as public safety, crime prevention or national security?
- Is the degree of interference proportionate to the pressing need?
  - For example, careful consideration will be used to ensure that the number of cameras, their location and use is proportionate to the threat or risk to public safety. The analysis of the perceived threat will also involve a careful examination of all available options capable of containing the risk with a view to selecting the least intrusive option or combination of options.
- Care must be taken to ensure that CCTV operators are comprehensively aware of the content of this Code of Practice and associated Procedure Manual as well as human rights principles

Arbitrary surveillance is to be avoided at all costs and CCTV operators will be expected to justify and defend any infringement of rights.

- 4.1 Operators must pay particular attention to the risk of infringing civil liberties. The Cayman Islands Government is committed to protecting the fundamental rights of individuals, including the right to privacy, and to avoid any infringements of those rights through the use of the National CCTV Programme.
- 4.2 Although technological safeguards are built into the National CCTV Programme, CCTV operators must be acutely aware of actions that could be considered an

infringement of privacy rights (e.g. attempting to look into the bedroom of a house, attempting to gain a close up of a person's anatomy, or of courting couples, etc.) Therefore, training of CCTV operators must ensure that they understand data protection principles and the obligations with respect to the right to privacy.

- 4.3 The guidelines included in this Code of Practice are based on best practice principles, and it is important that procedures in relation to the National CCTV Programme are fair and have integrity. This means that the Code may need to be updated periodically to take account of judicial rulings and advances in technology.
- 4.4 It is not intended that this document dictates or prescribes how individual CCTV systems are established. Although companies or individuals may have contributed funds towards the National CCTV Programme or linked their cameras to the system, there should not be, nor will there be, any preferences or rights given to such companies or individuals, including any right of access to the captured CCTV images.
- 4.5 All general and evidential images acquired by the National CCTV Programme shall only be used for the purposes stated at paragraph 1.2. If those stated purposes are expanded or amended at any point in the future, then this Code must be amended and a declaration made that the changes are fair, necessary and proportionate to their need.

#### 5. DATA PROTECTION

- 5.1 In due course, the use of CCTV will be regulated by a Data Protection Law. A Data Protection Committee is presently working on the preparation of a draft Bill. This legislation will prescribe how personal data shall be processed, including how images shall be obtained, retained and shared to ensure that CCTV surveillance is fair, necessary and proportionate to the stated aims of the system.
- 5.2 The forthcoming legislation will establish the use of the Office of the Information Commissioner, an independent body tasked with ensuring compliance with the legislation. Although the legislation will cover much more than data protection issues associated with CCTV, there will be important requirements placed on users and operators of CCTV systems. For example, all users and operators will be required to register with the Office of the Information Commissioner. Furthermore, the Office of the Information Commissioner will approve a CCTV Code of Practice to which all registered CCTV operators will be required to adopt.
- 5.3 The legislation will also carefully prescribe how images captured by CCTV are to be handled, retained and shared. The Code of Practice will provide recommendations and good practice advice on how the legal requirements of the legislation can be met.
- 5.4 Until the legislation comes into effect the principles contained in this Code of Practice, at clause 2.1.(iv) above, will be used.
- 5.5 When the Data Protection Law comes into force, this Code of Practice will be reviewed to determine that it meets the standards set out in the Data Protection Law. The revised version will also include a statement of compatibility with the Law. Further, the National CCTV Programme will have to be registered with the regulatory body identified under that Law. If the scheme becomes registered at any time after installation of the system, a statement to this effect should be included in the Annual Report for that year and added to the Code of Practice.

# 6. RESPONSIBILITY FOR THE SYSTEM

Responsibility for the day to day management of the National CCTV Programme rests with the CCTV Administrator. The functions of the CCTV Administrator are carried out by the Assistant Manager of the Electronic Monitoring Centre of the Cayman Islands Emergency Communications and Electronic Monitoring Department. This person reports to the Emergency Communications Manager of the Emergency Communications & Electronic Monitoring Department within the Portfolio of Internal and External Affairs.

# 7. CAMERA POSITIONING, COVERAGE AND SIGNAGE

- 7.1 The areas covered by the National CCTV Programme to which this Code of Practice refers are the public areas.
- 7.2 The camera sites should be determined on the recommendations of the RCIPS based on crime pattern analysis and other factors as per Section 1.2.
- 7.4 Cameras should be prominently situated in fixed positions within public view. No camera is to be hidden or obscured and, as far as possible, cameras should be beyond the risk of criminal damage.
- 7.5 From time to time transportable or mobile cameras may be temporarily located within the Cayman Islands. The use of such cameras, and the data produced by virtue of their use, will always accord with the objectives of the National CCTV Programme and be governed by this Code. Cameras will be sited using the following guidelines:
  - Cameras must only monitor those spaces intended to be covered.
  - Cameras must be situated to ensure that they will effectively capture images relevant to the scheme's purpose.
  - If there is a risk of neighbouring private spaces being monitored unintentionally the owner of such spaces will be consulted.
  - Adjustable cameras will be restricted to prevent operators from being able to allow unintended spaces to be viewed and/or recorded.
  - Cameras will be able to produce images of sufficient size, resolution and frames-per-second
  - Physical conditions and environment will be considered when siting cameras, for instance taking into account lighting and the size of the area to be viewed.
  - All necessary steps will be taken to protect the cameras from vandalism and theft.
- 7.6 Maximum deterrent value will be achieved by ensuring that cameras are clearly visible to members of the public.
- 7.7 Fair processing requires that individuals must be informed that their images are being captured. This will be in the form of signage. Signs should be placed so that the public are aware that they are entering a zone which is covered by surveillance equipment. The signs should be clearly visible and legible to the public. See Appendix B for an example of the Public CCTV System sign.
- 7.8 Compliant signs should contain the identity of the owners of the CCTV system, and details of whom to contact regarding the System. Signs will be sited using the following guidelines:
  - Signs will clearly identify to the public when they are entering an area covered by CCTV.

- These "boundary" signs may be supplemented with further signs inside the area if required.
- Signs will be clear and legible both in terms of lettering and size, and be appropriate to the sign's location.
- Signs will identify:
  - Who is responsible for the scheme
  - o The scheme's purpose
  - Details of who to contact about the scheme.
- 7.12 The use of covert processing, including the removal or failure to provide signs, is prima facie a breach of the fairness requirement. The installation of a CCTV camera is considered to be overt unless it is installed in a manner whereby its presence is deliberately intended to be concealed from the view of any person likely to be within the field of view of that camera.
- 7.13 However, an exception may arise where public CCTV surveillance is carried out specifically for the purposes of prevention or detection of crime and apprehension or prosecution of offenders, pursuant to an investigation being carried out by RCIPS and in keeping with its policy pertaining to covert surveillance. SUCH COVERT SURVEILLANCE IS NOT COVERED BY THIS CODE OF PRACTICE. At a minimum, however, where public CCTV cameras are to be used for covert purposes as part of a police investigation such use must be specifically authorized by a RCIP officer of the rank of Superintendent or above and be agreed by the Electronic Monitoring Centre Manager. In addition, only authorized, specially trained staff of the Electronic Monitoring Centre will be permitted to operate the cameras at such times. Comprehensive regulatory safeguards will be contained in the anticipated data protection legislation and any other legislation or subsidiary legislation regulating covert investigatory procedures.
- 7.14 Some cameras may be enclosed within 'all weather domes' for aesthetic or operational reasons but appropriate signs will identify the presence of all cameras. Cameras which may be placed in domes or covered to reduce the likelihood of assessing their field of view, or to protect them from weather or damage, will not be regarded as covert provided that appropriate signs indicating the use of such cameras are displayed in the vicinity.
- 7.16 Some of the cameras offer full colour, pan tilt and zoom (PTZ) capability, some of which may automatically switch to monochrome in low light conditions.
- 7.17 Some of the cameras will be capable of Automatic Number Plate Recognition which will photograph and record an image of a vehicle and its associated license plate. The plate number will be automatically updated to a database which will store the images, the camera number (location) and date/time the images were recorded.
- 7.18 As noted in 7.13, targeted surveillance is not covered by this Code and views into residential premises and office accommodations will as far as possible be excluded from the field of vision. Every effort must be made to prevent close up views into windows of living accommodations.
- 7.19 The CCTV Administrator will be responsible for putting in place a Procedure Manual containing the day-to-day instructions for operation of the Public CCTV System.

This Procedure Manual may be amended and developed whenever necessary to reflect changes in routine and practice. The Procedure Manual will contain

- a list of aims and objectives
- details of access to (and control of) monitoring areas
- the organisational structure and staffing of the Control Room
- requirements for record keeping
- information on the actions of operators
- · crime investigation records
- image management systems
- · record partnership protocols
- legislation updates
- notes on the development of the CCTV system.

Any part of this Code of Practice which is procedural in nature will be reproduced and expanded upon if necessary in the Procedure Manual.

# 8. CONTROL, MONITORING AND OPERATION OF CAMERAS

- 8.1 A staffed monitoring room is located at the Cayman Islands Electronic Monitoring Centre (CIEMC), George Town, Grand Cayman.
- 8.2 Secondary monitoring equipment may be located in RCIPS premises, at the Cayman Islands Emergency Communications Centre (CIEC911) and at the National Emergency Operations Centre (NEOC). No equipment, other than that operated by staff at the Cayman Islands Electronic Monitoring Centre shall be capable of recording images from any of the cameras (with the exception of Cayman Brac which shall be recorded at the Cayman Brac RCIPS Station).
- 8.3 The CCTV Administrator will hold responsibility for managing the monitoring, operation and evaluation of images captured by the National CCTV Programme and compliance with this Code of Practice. The monitoring and operation of cameras located on Cayman Brac shall be the responsibility of the RCIPS Cayman Brac District Officer in Charge.
- 8.4 The CCTV Administrator shall also be responsible for maintaining full management information as to the incidents dealt with by the Electronic Monitoring Centre, for use in the management of the system and in future evaluations.
- 8.5 Unauthorized persons will not have access to the Electronic Monitoring Centre or CCTV equipment based at a secondary monitoring site without an authorized member of staff being present. A list of authorized personnel is attached at Appendix D.
- 8.6 The Electronic Monitoring Centre shall be staffed by specially selected and trained personnel in accordance with the strategy and principles contained within the Procedures Manual and any current or subsequent relevant legislation regarding the recruitment, training and supervision of security type personnel.
- 8.7 All operators shall receive training relevant to their role. Further training will be provided as necessary and in particular further training will be provided on legislation being brought into force subsequent to the publication of this code.
- 8.8 Electronic Monitoring Centre personnel will be able to record images from selected cameras in real-time, produce hard copies of recorded images, replay or copy any pre-recorded data at their discretion and in accordance with the Code of Practice. All viewing and recording equipment shall only be operated by trained and authorized users.
- 8.9 The RCIPS will respond, where possible to information provided by Electronic Monitoring Centre personnel which requires RCIPS action.
- 8.10 It cannot be guaranteed that all offences will be detected even when a captured CCTV image of suspect(s) is available. Equally, it cannot be guaranteed that where an offence has occurred, that captured CCTV images of that offence will be available.

Consequently, the Cayman Islands Government will not be liable for any loss, damage, or injury that occurs within the areas that are monitored.

- 8.11 If not carefully managed, RCIPS' use of the system may extend into ways not foreseen when the scheme was established and the Code of Practice adopted. It is important to preserve best practices and efficient management of the scheme that it should not be used to obtain recorded visual evidence to monitor or prosecute minor street offences unless accompanied by a more serious offence, or unless such minor offence is of a nature that causes public danger or serious nuisance.
- 8.12 The use of a Public CCTV System to obtain recorded visual evidence in relation to other non-serious offences will be guided by the RCIPS standard operating guidelines, RCIPS' priorities, guidance from the Attorney General and other public interest considerations.
- 8.13 Except where used for training of persons involved with the National CCTV Programme, there should be no public viewing of the monitors. There must be careful selection of any material to be used for such purposes to ensure data protection principles are not breached. Further, under no circumstances will recorded material be released for commercial sale for any purpose.
- 8.14 Where monitoring is done at both the Electronic Monitoring Centre and at a secondary monitoring location, recordings will only be made at the Electronic Monitoring Centre. This is to ensure that only one recording is made. The monitoring equipment at a police station will not be capable of recording and/or storing captured images.
- 8.15 Where the RCIPS' uses any aspect of the Public CCTV System from outside the Electronic Monitoring Centre, without making direct contact with the Electronic Monitoring Centre, means should be devised to ensure that records are kept which meet the requirements of the Code of Practice and are subject to audit.
- 8.16 Any person operating the cameras will act with utmost probity at all times.
- 8.17 The cameras, control equipment, recording and reviewing equipment shall at all times only be operated by persons who have been trained in their use and the implications of their use.
- 8.18 Every use of the cameras will accord with the purposes and key objectives of the System and shall be in compliance with this Code of Practice.
- 8.19 Cameras will not be used to look into private residential property. 'Privacy zones' shall be programmed into the System (whenever possible) or other electronic means of masking out private areas will be used in order to ensure that the interior of any private residential property within range of the System is not surveyed by the cameras. If it is not possible to do either of the above, there is to be full consultation with the owner of such property before such cameras are used.
- 8.20 Camera operators will be mindful of exercising prejudices which may lead to complaints of the System being used for purposes other than those for which it is intended. Operators may at any time be required by the CCTV Administrator or during

an audit to justify their interest in, or recording of, any particular individual, group of individuals or property.

8.21 Only those trained and authorized members of staff with responsibility for using the CCTV equipment will have access to the operating controls; those operators have primacy of control at all times.

#### 9. STAFF AND TRAINING

- 9.1 Persons working in the Electronic Monitoring Centre and others authorised to operate CCTV cameras must meet the highest standards of professionalism and integrity. These qualities must be carefully considered when staff members are being recruited.
- 9.3 A failure to comply with the procedures set out in the Procedure Manual may give rise to disciplinary action in accordance with the Public Service Management Law (2010 Revision).
- 9.4 To achieve the maximum potential from the Public CCTV System, it is critically important that operators are able to identify suspicious behaviour, make informed decisions when to track individuals and groups, and when to take close up views of incidents or people. Training is therefore highly important and it is insufficient to assume that these skills are self evident or may be left to common sense. Such training must also teach operators that the process of identifying suspicious behaviour must avoid influence based on discrimination, either consciously or unconsciously, on the grounds of aspects outlined in the Constitution, namely sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, age, mental or physical disability, property, birth or other status.
- 9.5 Equipment associated with the System will only be operated by authorized personnel who will have been properly trained in its use and all monitoring room procedures as set out in the Procedure Manual.
- 9.6 Every person involved in the management and operation of the System will be personally issued with a copy the Code of Practice, and will be required to sign a confirmation that they fully understand the obligations adherence to the Code of Practice and Procedure Manual places upon them and that any breach will be considered as a disciplinary offence.
- 9.7 Every individual with any responsibility under the terms of this Code of Practice and who has any involvement with the System to which they refer, will be subject to the Cayman Islands Civil Service Code of Conduct and Workplace Rules. Any breach of this Code of Practice or of any aspect of confidentiality will be dealt with in accordance with those disciplinary rules.
- 9.8 The Emergency Communications Manager of the Emergency Communications and Electronic Monitoring Department will accept primary responsibility for ensuring that there is no breach of security and that the Code of Practice is complied with. The Emergency Communications Manager may delegate day to day responsibility for the management of the Electronic Monitoring Centre and for enforcing the disciplinary rules to the Assistant Manager Electronic Monitoring Centre. Non-compliance with this Code of Practice by any person will be considered a severe breach and will be dealt with accordingly, including, if appropriate, the instigation of criminal proceedings.

9.9 Every indivand who has any confidentiality.	vidual with any responsibility under the terms of this Code of Practice involvement with the System, will be required to sign a declaration of

# 10. GENERAL RECORDED DATA

- 10.1 Recorded data shall be divided into General and Evidential.
- 10.2 General recorded data will be retained for a maximum of 60 days. On the 61<sup>st</sup> day any recorded raw video that has not been copied onto another media for an authorized request will be deleted automatically by the Video Management Software.
- 10.3 There should be no public access to either Evidential or General recorded data except where the applicant is a victim, complainant or suspect, involved in a criminal offence recorded by the System. Access must be strictly controlled and supervised and will be given on the advice of the Attorney General or his/her authorised representative.
- 10.4 Recorded data may, on occasions and at the discretion of the Electronic Monitoring Centre manager be used for training of Public CCTV System operators or demonstration purposes. Under no circumstances will recorded material be released for commercial for any purpose.
- 10.6 Access to recorded data must adhere fully to the Code of Practice.

#### 11. EVALUATION

- 11.1 The Electronic Monitoring Centre will keep a record of all arrests and notable incidents that were assisted by the use of the CCTV System.
- 11.2 A statistical report should be produced initially on a six-month basis for the first two years and annually thereafter. It should include the numbers of arrests and notable incidents by date and type that have been assisted by the CCTV System.
- 11.3 The report should also include an analysis of the technical performance of the CCTV System and possibly a cost benefit analysis of the CCTV System.
- 11.4 The number and the type of complaints that have been attributed to the System should be outlined, of these complaints, the number substantiated should be shown and the actions taken to remedy them.
- 11.5 Statistical analysis should be carried out by the RCIPS on crime and incident trends -- in particular on how it might appear that the Introduction of the CCTV System has affected neighboring areas, e.g. the various categories of crime displacement, or diffusion of benefit (i.e. non-CCTV areas usually near to areas covered by CCTV, that also appear to reap the benefits of crime prevention and reduction).
- 11.6 The RCIPS should then make the information derived from the statistical analysis available to the Portfolio of Internal & External Affairs.
- 11.7 The Portfolio of Internal & External Affairs shall be responsible for ensuring that effective independent evaluation of the CCTV System is undertaken periodically. This should include as a minimum:
  - (a) Assessment of impact upon crime
  - (b) Assessment of neighbouring areas without CCTV
  - (c) The views of the public
  - (d) Operation of the Code of Practice
  - (e) Whether the purpose for which the scheme was established still exists and if not, would the removal of the CCTV System cause a return of crime to the area.

Evaluations or assessments of the National CCTV Programme will include discussion, at least in general terms, of any complaints or reports of breaches of security or of this Code of Practice. In addition, the use of images or information gained from the National CCTV Programme will be tracked by staff to ensure that the images and equipment are not only being used appropriately, but that there is maintained an informal log of successes due to the CCTV Programme (such as arrests, charges, convictions etc) that will prove 'value for money'.

11.8 The result of the evaluation should be published and taken into account in the future functioning, management and operation of the system. A monitoring and evaluation group should he established with the remit to continuously evaluate the system.

# 12. EVIDENCE

- 12.1 Evidence in relation to CCTV is potentially anything that has been recorded by the CCTV System.
- 12.2 Any description of suspects and offenders, if passed directly to the Electronic Monitoring Centre from the Emergency Communications Centre or the original source via telephone, radio or any other means must be entered on the Electronic Monitoring Centre Log.
- 12.3 Where a CCTV System user is viewing an incident or suspected crime it will be necessary to record the description of the suspect.
- 12.4 The Electronic Monitoring Centre's Log should be retained as an exhibit, and be produced with statements if they form part of the evidence in a case. The private information of individuals not concerned with the case will be redacted from the exhibited log.
- 12.5 The copying of recorded data should only be carried out by a trained Electronic Monitoring Center staff member who shall record the fact in writing and, where appropriate, produce the record with a written statement. Actions to ensure Continuity of Evidence are essential.
- 12.6 Recordings should not be shown to any unauthorized person(s) even if the incident relates to an alleged crime and the recording is likely to be used as evidence in court.

#### 13. EVIDENTIAL RECORDED MATERIAL

- 13.1 Electronic Monitoring Officers, Electronic Monitoring Supervisors and the Assistant Manager Electronic Monitoring Centre should use their judgment and discretion to initiate the identification of images that may have evidential value. In such cases two copies of the data will be placed on a CD/DVD (Read Only) or other approved media. Both copies will be initialed in ink by the Electronic Monitoring Centre staff member who initiated the recording copy. One copy will be sent to the RCIP or other authorized agency for follow up. The second will be retained at the Electronic Monitoring Centre in secured storage. Both copies must be clearly and uniquely labeled, sealed and treated as evidence.
- 13.2 Copies of recorded material shall only be retained by the Electronic Monitoring Centre until a court has given a judgment and all appeal options have been exhausted. Where the copy is of material forwarded to another authorized agency, it will be retained by the Electronic Monitoring Centre until such time as notified by the agency that it may be destroyed. Where such notification is not received the Electronic Monitoring Centre must contact the agency concerned every six months and request a certificate from the agency that the recorded material is still required for evidential purposes. Any failure by the authorized agency to provide such certification within thirty days of the request will cause the destruction of the copy held by the Electronic Monitoring Centre.
- 13.3 Once in the possession of the RCIP the recorded images shall be subject to existing protocols or policies on handling and storing evidential material. Existing procedures should be used to document the viewing or movement of copies of the recordings. If it is necessary to break the security seal on the CD-ROM, the reason must be properly documented and the seal replaced as soon as possible.
- 13.4 Where any recording that may contain evidence is the property of any third party, a copy of the recording should be made and provided to the RCIPS. If the third party's CCTV system is capable of being recorded by the Electronic Monitoring Centre, a second CD/DVD shall be retained in secured storage, uniquely labeled, sealed and treated as evidence. Its retention will be on the same basis as set out in 13.2 above. In all cases the recorded copy must be in a Read Only format.
- 13.5 If it is necessary to produce additional copies of a recording for judicial proceedings, a record must be kept in the Electronic Monitoring Centre Log of how many certified copies have been made, their reference number and who has possession of them. Copies should only be made for evidential purposes, and should only be made available to the RCIPS, the Attorney General, defence solicitors and other prosecuting authorities. Each copy shall be individually marked. Copies can only be reproduced by the CCTV Administrator or under his direction or by permission of the Attorney General or his appointed representative.
- 13.6 No copy of a recording held by the Electronic Monitoring Centre will be disposed of without first being electronically wiped or destroyed. All additional copies produced for evidential purposes must be returned to the Electronic Monitoring Centre upon request where they will be destroyed and a record of their destruction retained.

- 13.7 With respect to the logging of information this log shall be in electronic format with security features and shall be maintained for:
  - (i) all requests for copies of images along with information concerning who made the copy, how it was distributed and to whom; and
- (ii) individual requests for copies to establish a chain of custody for the image copy.

#### 14. IDENTIFICATION PROCEDURES

- 14.1 In all cases it is a matter of the utmost importance that the description of a suspect as "first given" must be recorded
- 14.2 In cases involving the evidence of CCTV especially where the initial evidence or beginning of an incident has been viewed by remote camera(s) in the first instance, the preservation of the recording and its security, are paramount.
- 14.3 An investigating officer may show a video or still image of an incident to the public at large for the purpose of recognizing or tracing suspects. Care must be taken however to ensure that prior to release, video and still frames are edited so as to protect the identity of data subjects who are not under any reasonable suspicion but who appear in the captured video or still frame coincidentally.
- 14.4 An officer may also show such video footage or still images to RCIPS Officers or civilian witnesses for the purpose of recognizing and tracing suspects. Again, such video footage or still images must not allow persons not under suspicion to be identifiable.

#### 15. MEDIA

- 15.1 Under no circumstances will copies of recorded data be passed to or made available to the media, except with the approval of the CCTV Administrator in consultation with the RCIPS or persons designated with this authority.
- 15.2 Where recorded data relates to a suspected criminal offence and its release to the public via the media, including television, is desirable for the purposes of identifying witnesses or suspects, authority must first be obtained from the Commissioner of Police or persons designated with this authority.
- 15.3 CCTV footage may be shown to members of the public, including at local trade and business events, as a marketing tool to raise funds through sponsorship or other means. However, prior to such use, persons identifiable in the footage must give their consent or, where the number of persons shown in the footage is too great to make this practical, then their identities must be masked electronically.
- 15.4 Recorded data may be viewed by anybody carrying out an independent evaluation of the scheme. Checks must first be undertaken prior to any evaluation that the individual or business entity employed to perform such evaluation is properly qualified for that purpose.

#### 16. ACCOUNTABILITY AND COMPLAINTS

- 16.1 Copies of the Code of Practice and particulars of the complaints system should be made readily available to the public.
- 16.2 Information must be published about the manner in which an individual can make a complaint about any aspect of the Public CCTV System. Information must be made available as to how to make a complaint, e.g. the name and address of the person to whom the complaint should be made, and their responsibility in handling the complaint. This information should also state that complaints will be responded to with the minimum delay and at a minimum within the timeframe specified for responding to requests for information under the Freedom of Information Law.
- 16.3 The Annual Report shall include information on the number of complaints received, how many were substantiated and any action taken to remedy the complaint.
- 16.4 All alleged breaches of this Code of Practice must be investigated thoroughly by the Portfolio of Internal and External Affairs. Where a breach is confirmed, systemic changes must be instituted immediately so as to avoid any future reoccurrence. Breaches of the Code may also give rise to disciplinary action against persons involved in operating the National CCTV Programme or those who have access to material recorded from it. The results of any investigation would not as a matter of practice be released to the public either in line with normal human resources policies or in response to a FOI request.

# 17. ACCESS TO THE ELECTRONIC MONITORING CENTRE

- 17.1 Access to the Electronic Monitoring Centre, whether to view monitors, or to operate equipment, should be limited to the authorized personnel who are trained and authorised to operate the system.
- 17.2 When the Electronic Monitoring Centre is unstaffed, it will be properly secured. Operational safeguards must also be implemented to ensure the integrity of the recordings at all times.
- 17.3 All visitors must be accompanied by an employee of the Electronic Monitoring Centre at all times and at no time should they be left unattended.

# 18. FREEDOM OF INFORMATION LAW

18.1 National CCTV Programme is not subject to the FOI Law as images are being recorded for the purpose of assisting the RCIPS in intelligence-gathering (per The Freedom of Information Law, 2007 Section 3 Paragraph (5)(b).

# CAYMAN ISLANDS GOVERNMENT CCTV CODE OF PRACTICE APPENDIX A – NATIONAL CCTV MASTER CAMERA LIST

# **Bodden Town**

Anton Bodden Drive / Verneice Bodden Drive Phase 2+ Bodden Town Road / Anton Bodden Drive Phase 1 Bodden Town Road / Cumber Avenue Phase 1 Hirst Road / East West Arterial Highway Phase 1 Shamrock Road / Beach Bay Rd. Phase 1 Shamrock Road / Bougainvillea Way Phase 2+ Shamrock Road / Condor Road Phase 1 Shamrock Road / Hirst Road Phase 1 Shamrock Road / Jayson Avenue Phase 1 Shamrock Road / Northward Road Phase 1

# Cayman Brac

Ashton Reid Drive / Songbird Drive Phase 2+ Bert Marson Drive / South Side West Road Phase 2+ Captain Mabry Drive / Heights Road Phase 2+ Dennis Foster Road / Ashton Reid Drive Phase 2+ Dennis Foster Road / Coastal Way Phase 2+ Hemmington Road / Bluff West Road Phase 2+ Hemmington Road / Songbird Drive Phase 2+ Rock Road / Harold Drive Phase 2+ South Side East Road / Sunshine Drive Phase 2+ South Side West Road / Ashton Reid Drive Phase 2+ Phase 2+ Spot Bay Road / Lighthouse Road Sunshine Drive / Major Donald Drive Phase 2+ Watering Place Road / Plaza Drive Phase 2+ West End East Road / Cemetery Road Phase 2+ West End West Road / Cross Road Phase 2+

# East End

John Maclean Drive / Farm Road Phase 1
Sea View Road / Eastland Drive Phase 1
Sea View Road / John Maclean Drive Phase 1

# **George Town**

Bobby Thompson Way / Linford Pearson Highway	Phase 1
Bobby Thompson Way / Smith Road	Phase 1
Crewe Road / Lyndhurst Ave.	Phase 1
Crewe Road / Ryan Road	Phase 2+
Crewe Road / Tropical Gardens Road	Phase 1
Cypros Road / Greenwood Drive	Phase 2+
Dorcy Drive / Owen Roberts Drive	Phase 1
Dorcy Drive / Portland Road	Phase 2+
East West Arterial Highway / Poindexter Road	Phase 1
Easterly Tibbetts Highway / Dump	Phase 2+
Easterly Tibbetts Highway / Gecko Link	Phase 2+
Easterly Tibbetts Highway / Lawrence Boulevard	Phase 2+
Easterly Tibbetts Highway / Nexus Way	Phase 2+
Eastern Avenue / Bodden Road	Phase 1
Eastern Avenue / Godfrey Nixon Way	Phase 1
Eastern Avenue / School Road	Phase 1
Eastern Avenue / Shedden Road	Phase 1
Eastern Avenue / Washington Road	Phase 1
Eastern Avenue / Watlers Drive	Phase 1
Edward Street / Cardinall Avenue	Phase 2+
Edward Street / Doctor Roys Drive	Phase 2+
Elgin Avenue / Hospital Road	Phase 1
Esterley Tibbetts Highway / Godfrey Nixon Way	Phase 1
Fairbanks Road / Outpost Street	
Harbour Drive / Cardinall Avenue	Phase 1

Harbour Drive / Fort Street	Phase 2+
Linford Pearson Highway / Halifax Road	Phase 2+
Linford Pearson Highway / Old Crewe Road	Phase 1
Mary Street / Fort Street	Phase 2+
Mary Street / Rock Hole Road	Phase 1
McField Lane / School Road	Phase 1
North Church Street / Bodden Road	Phase 2+
North Church Street / Mary Street	Phase 2+
North Sound Road / Dorcy Drive	Phase 1
North Sound Road / Shedden Road	Phase 1
North Sound Road / Sound Way	Phase 2+
North Sound Road / Sparkys Drive	Phase 2+
Shamrock Road / Bimini Drive	Phase 1
Shamrock Road / Crewe Road	Phase 1
Shamrock Road / East West Arterial Highway	Phase 1
Shamrock Road / Marina Drive	Phase 2+
Shamrock Road / Soto Lane	Phase 2+
Shamrock Road / Spotts Newlands Road	Phase 1
Shedden Road / Doctor Roys Drive	Phase 2+
Shedden Road / Edward Street	Phase 2+
Shedden Road / Linwood Road	Phase 2+
Shedden Road / Martin Road	Phase 1
Shedden Road / Mary Street	Phase 2+
Shedden Road / Tigris Street	Phase 2+
Smith Road / Anthony Drive	Phase 1
Smith Road / Hospital Road	Phase 1
South Church Street / Boilers Road	Phase 2+
South Church Street / Goring Avenue	Phase 2+
South Sound Road / Anne Bonnie Crescent	Phase 2+
South Sound Road / Old Crewe Road	
Walkers Road / Academy Way	Phase 1
Walkers Road / Schools	Phase 1

Walkers Road / South Sound Road	Phase 1
Walkers Road / Windsor Park Road	Phase 1
West Bay Road / Canal Point Drive	Phase 2+
West Bay Road / Eastern Avenue	Phase 2+
West Bay Road / Gecko Link	Phase 1
West Bay Road / Helen Drive	Phase 1
West Bay Road / Lawrence Boulevard	Phase 2+
West Bay Road / Safehaven Drive	Phase 2+
West Bay Road / Whitehall Gardens	Phase 2+
North Side	
Bodden Town Road / Frank Sound Road	Phase 1
Frank Sound Road / Bodden Town Road	Phase 1
North Side Road / Frank Sound Road	Phase 1
Rum Point Drive / Hutland Road	Phase 1
Rum Point Drive / Water Cay Road	Phase 1
West Bay	
Birch Tree Hill Road / Conch Point Road	Phase 1.1
Birch Tree Hill Road / Finch Drive	Phase 1.1
Boatswain Bay Road / Finch Drive	Phase 1.1
Conch Point Road / Captain Reginald Parsons Drive	Phase 1.1
Esterley Tibbetts Highway / Lime Tree Bay	Phase 1.1
Hell Road / Fountain Road	Phase 1.1
Hell Road / Miss Daisy Lane	Phase 1.1
Hell Road / Town Hall Road	Phase 1
Mount Pleasant Road / Captain Reginald Parsons Drive	Phase 1.1
North West Point Rd / Boatswain Bay Road	Phase 1
North West Point Road / Bonaventure Road	Phase 1.1
North West Point Road / Town Hall Road	Phase 1.1
North West Point Road / Watercourse Road	Phase 1.1
Rev Blackman Road / Mount Pleasant Road	Phase 1.1

Rev Blackman Road / Stadium Road	Phase 1.1
Rev Blackman Road / West Church Street	Phase 1.1
Stadium Drive / Birch Tree Hill Road	Phase 1
Watercourse Road / Hell Road	Phase 1.1
West Bay Road / Cemetery Road	Phase 1.1
West Bay Road / Governors Way	Phase 1.1
West Bay Road / Lime Tree Bay Avenue	Phase 1.1
West Bay Road / Raleigh Quay	Phase 1
West Bay Road / West Church Street	Phase 1
West Bay Road / Willie Farrington Drive	Phase 1.1
West Bay Road / Yacht Drive	Phase 1.1
Willie Farrington Drive / Batabano Road	Phase 1



# CAYMAN ISLANDS GOVERNMENT CCTV CODE OF PRACTICE APPENDIX C – PRIMARY AND SECONDARY MONITORING LOCATIONS

# **Primary Monitoring Location**

# **Cayman Islands Electronic Monitoring Centre (CIEMC)**

George Town Grand Cayman

# **Secondary Monitoring Locations**

# **Cayman Islands Emergency Communications Centre (CIEC911)**

George Town Grand Cayman

# **George Town Police Station (GTPS)**

69-A Elgin Avenue George Town Grand Cayman

# **Bodden Town Police Station (BTPS)**

445-B Bodden Town Road Bodden Town Grand Cayman

# **Cayman Brac Police Station (CBPS)**

9 Ivory Lane Cayman Brac

# **West Bay Police Station (WBPS)**

242 West Church Street West Bay Grand Cayman

# **National Emergency Operations Centre (NEOC)**

Airport Fire Station 148 Owen Roberts Drive George Town Grand Cayman

# CAYMAN ISLANDS GOVERNMENT CCTV CODE OF PRACTICE APPENDIX D – LIST OF AUTHORIZED CCTV OPERATORS

## The following posts are authorised to operate cameras and view images obtained thru the National CCTV Programme:

1. Members of the Emergency Communications Centre and Electronic Monitoring Centre – with the exception of administrative staff.

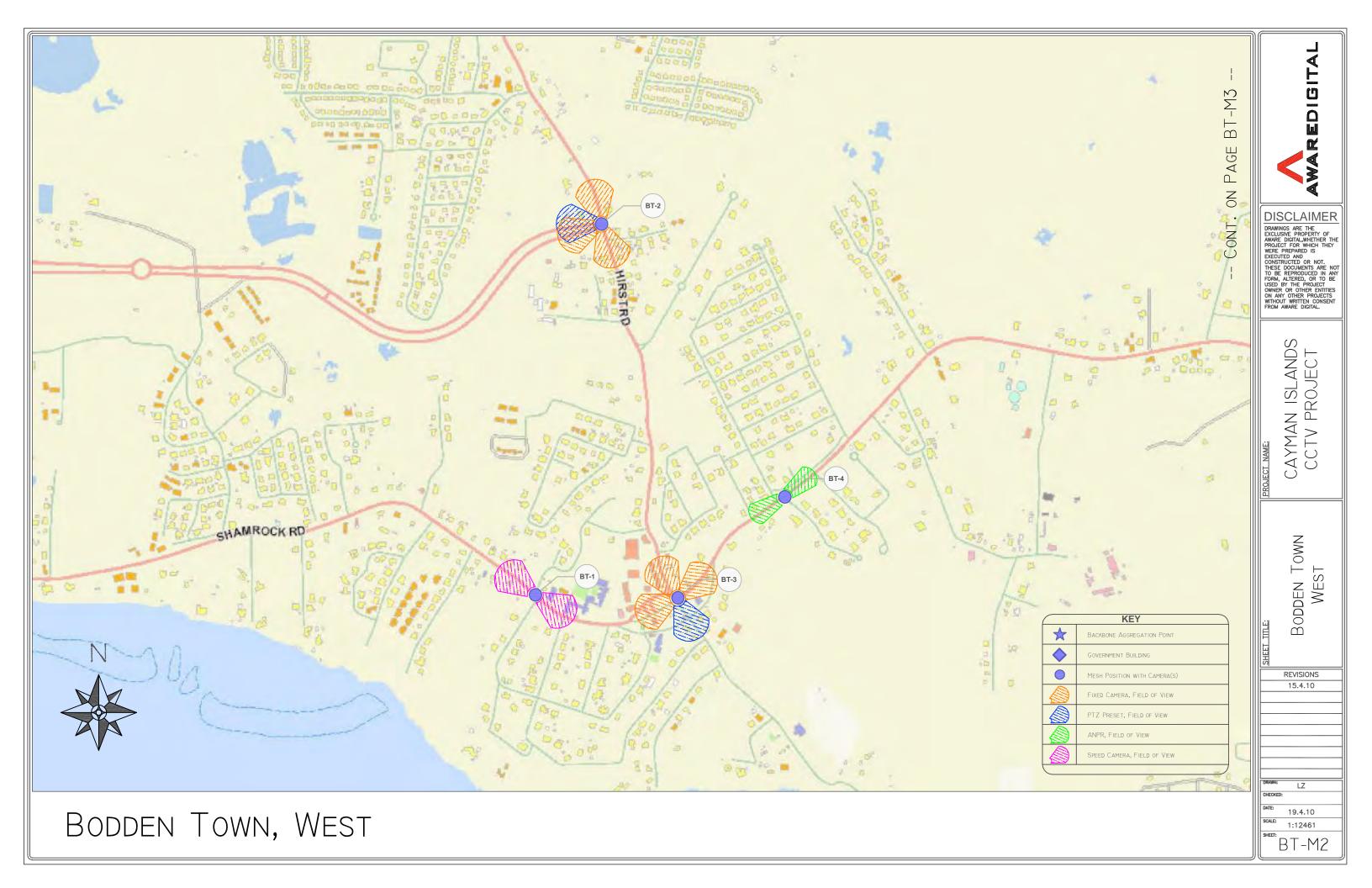
### The following posts are authorised to view images obtained thru the National CCTV Programme:

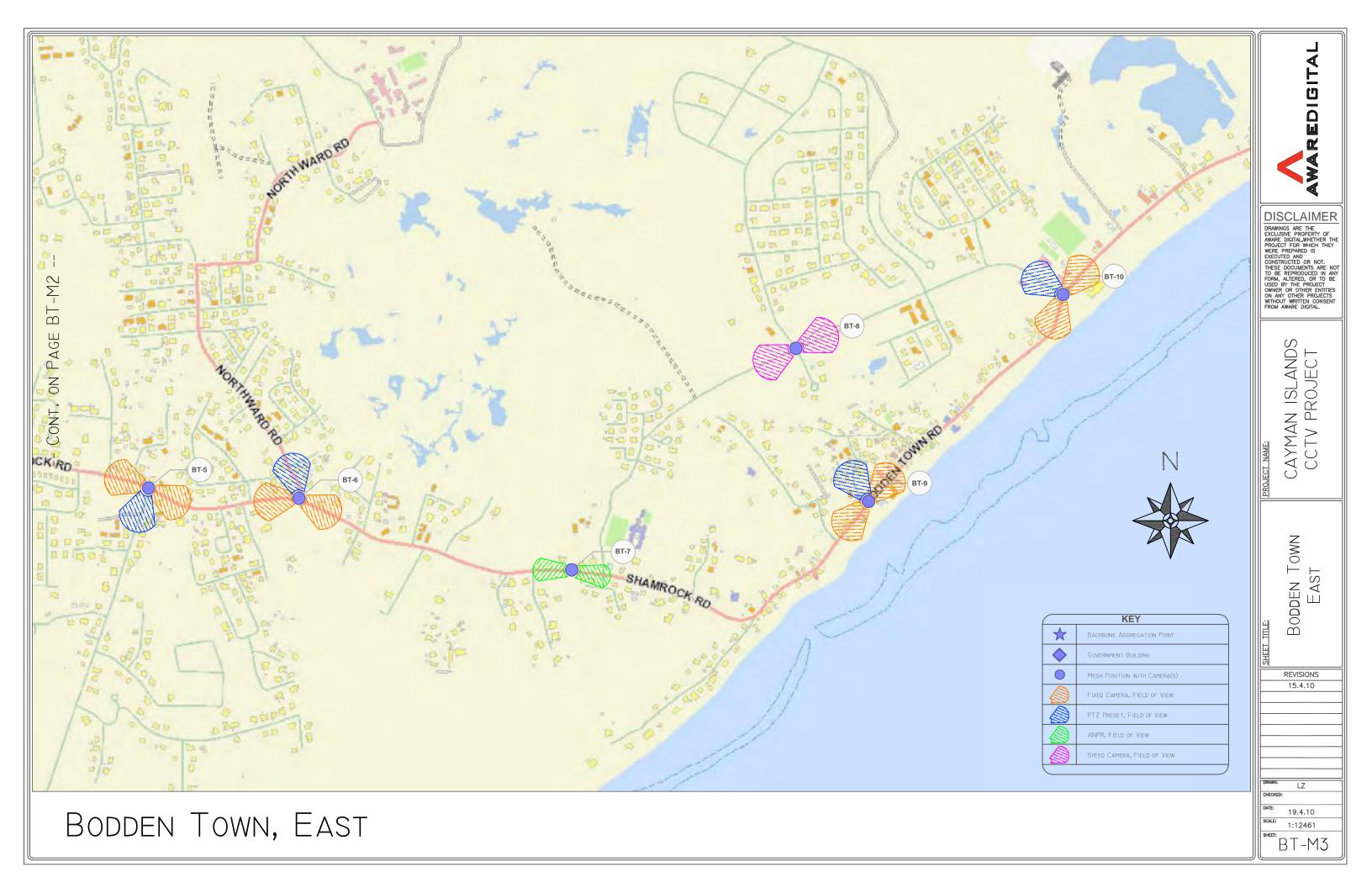
- 1. H.E. the Governor
- 2. Hon. Deputy Governor
- 3. Chief Officer Portfolio of Internal & External Affairs
- 4. Deputy Chief Officer (Uniform Division) Portfolio of Internal & External Affairs
- 5. Administrative Staff Emergency Communications & Electronic Monitoring
- 6. Members of the NEOC (during an activation)
- 7. Police Constables and above
- 8. Legal Department Members
- 9. Any other person authorized by the Manager of the Emergency Communications and Electronic Monitoring Center.

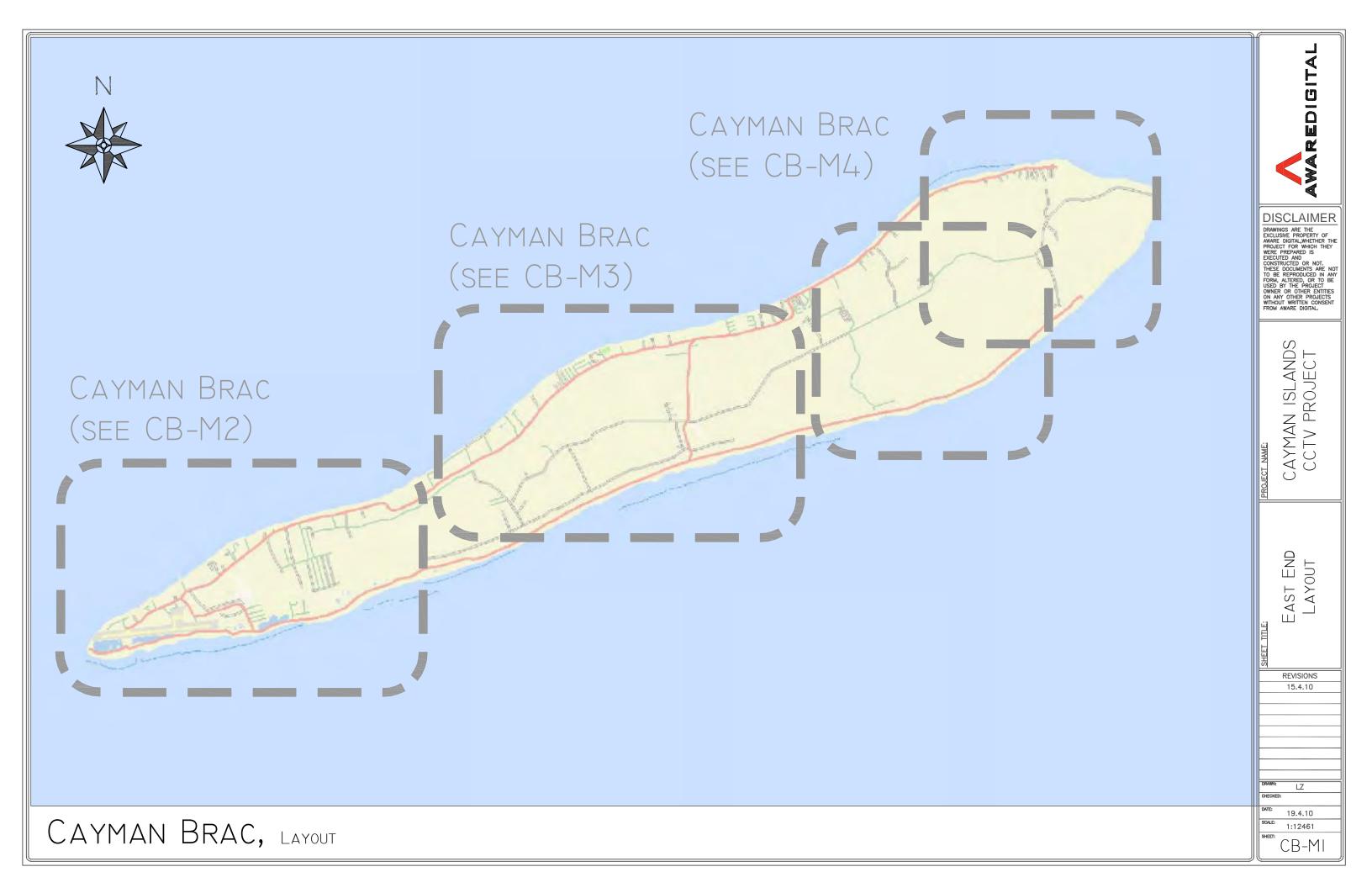
#### CAYMAN ISLANDS GOVERNMENT CCTV CODE OF PRACTICE APPENDIX E – CAMERA LOCATION MAP

- 1. Bodden Town
- 2. Cayman Brac
- 3. East End
- 4. George Town
- 5. North Side
- 6. West Bay



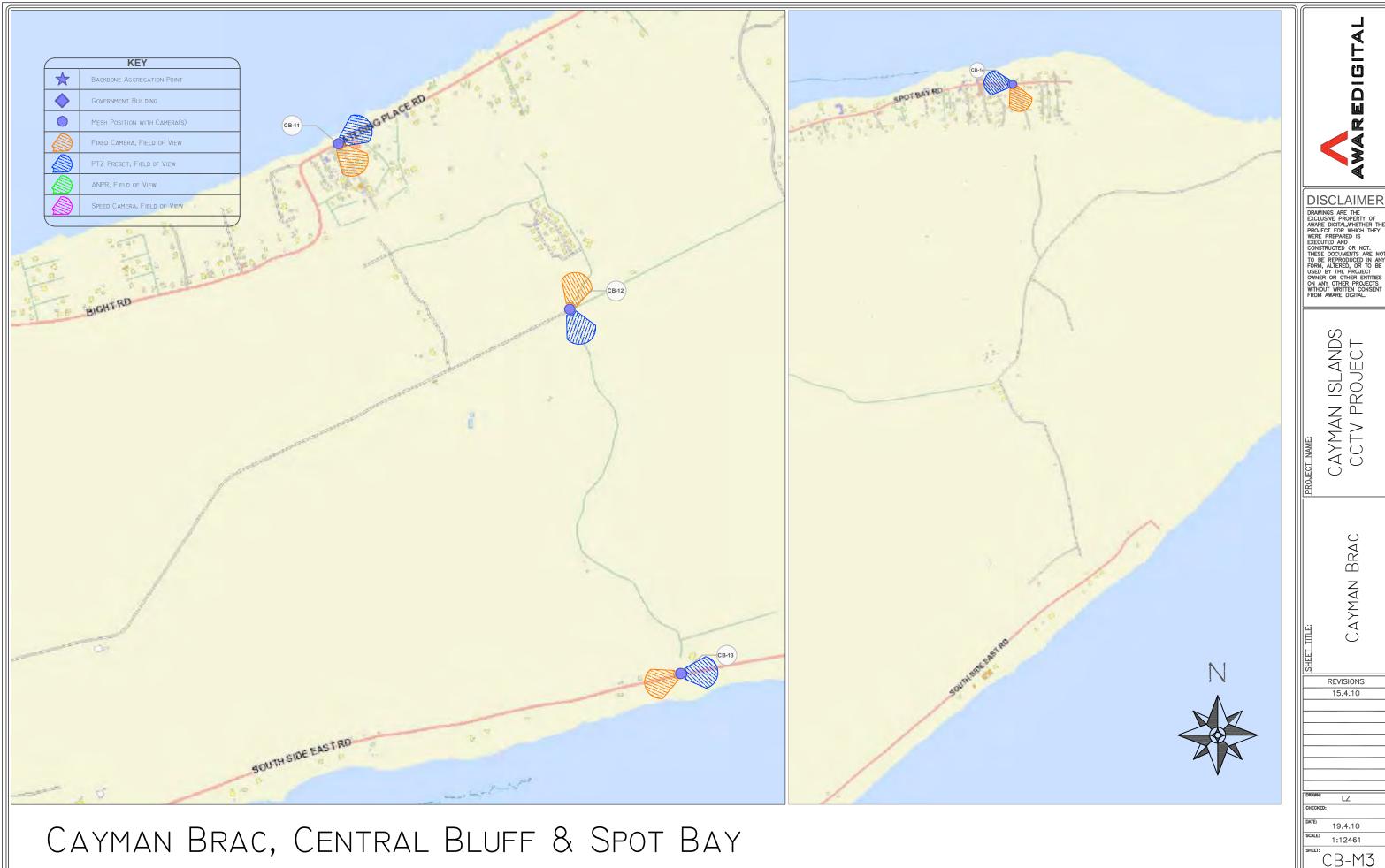




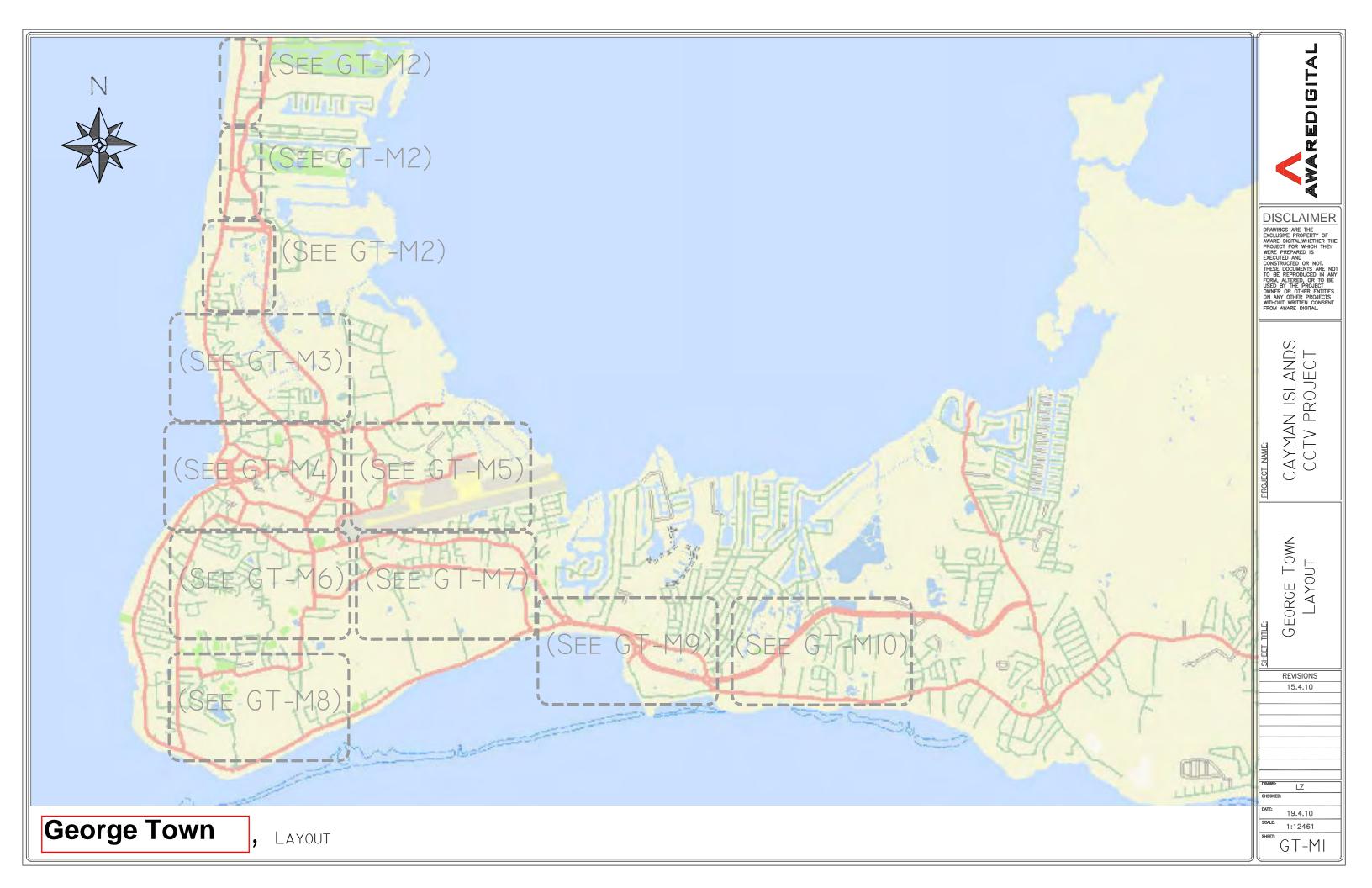


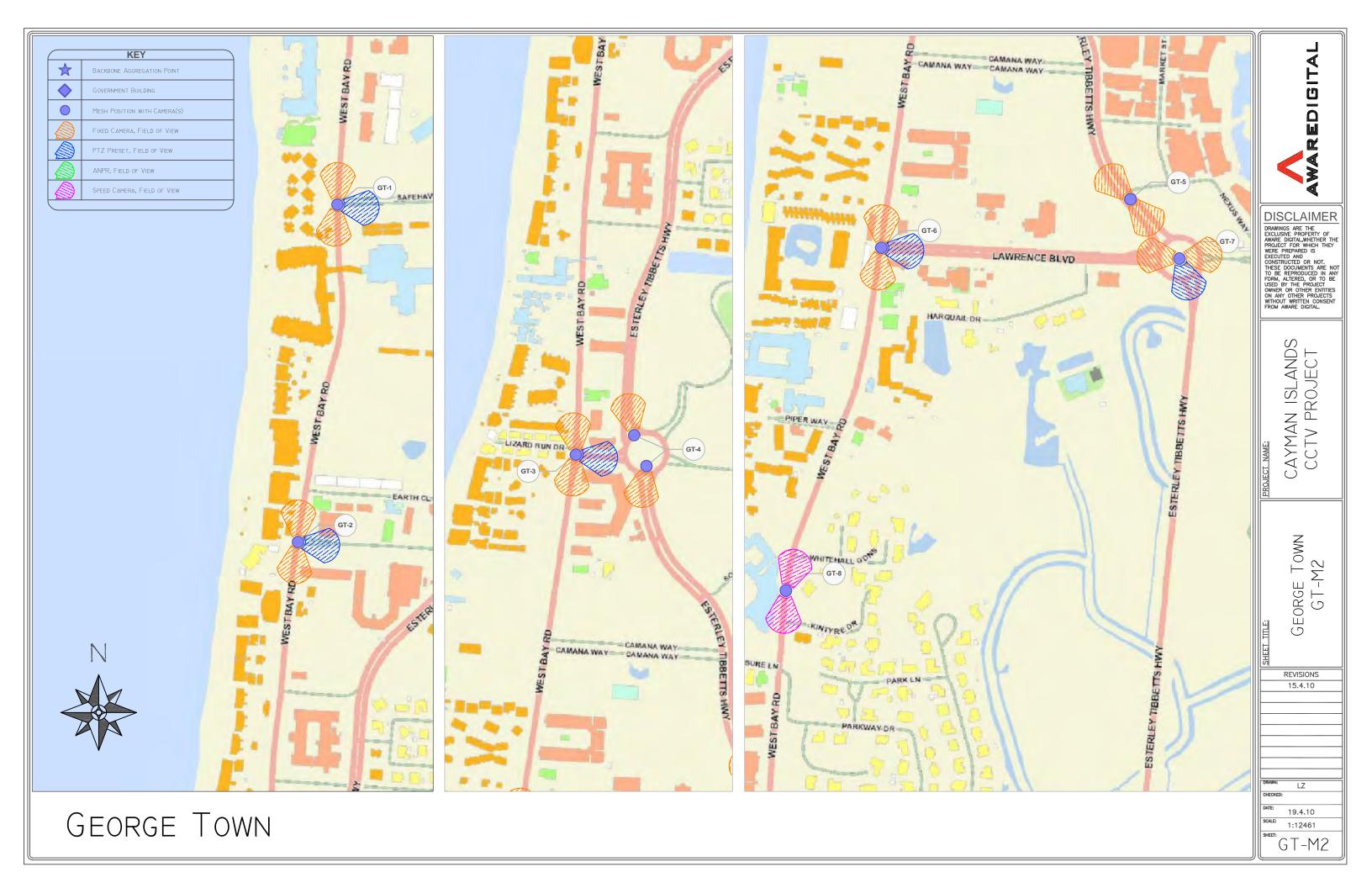


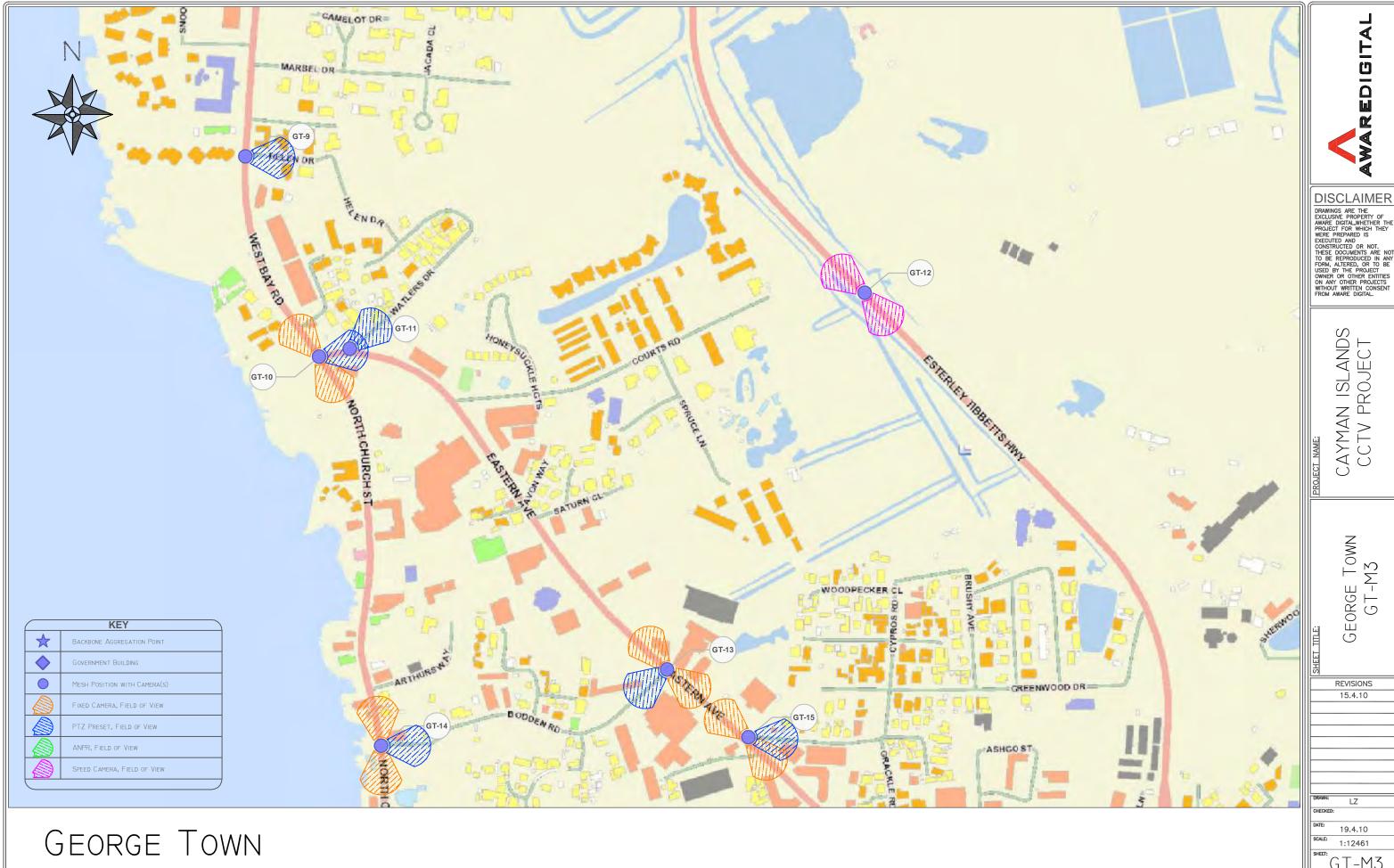




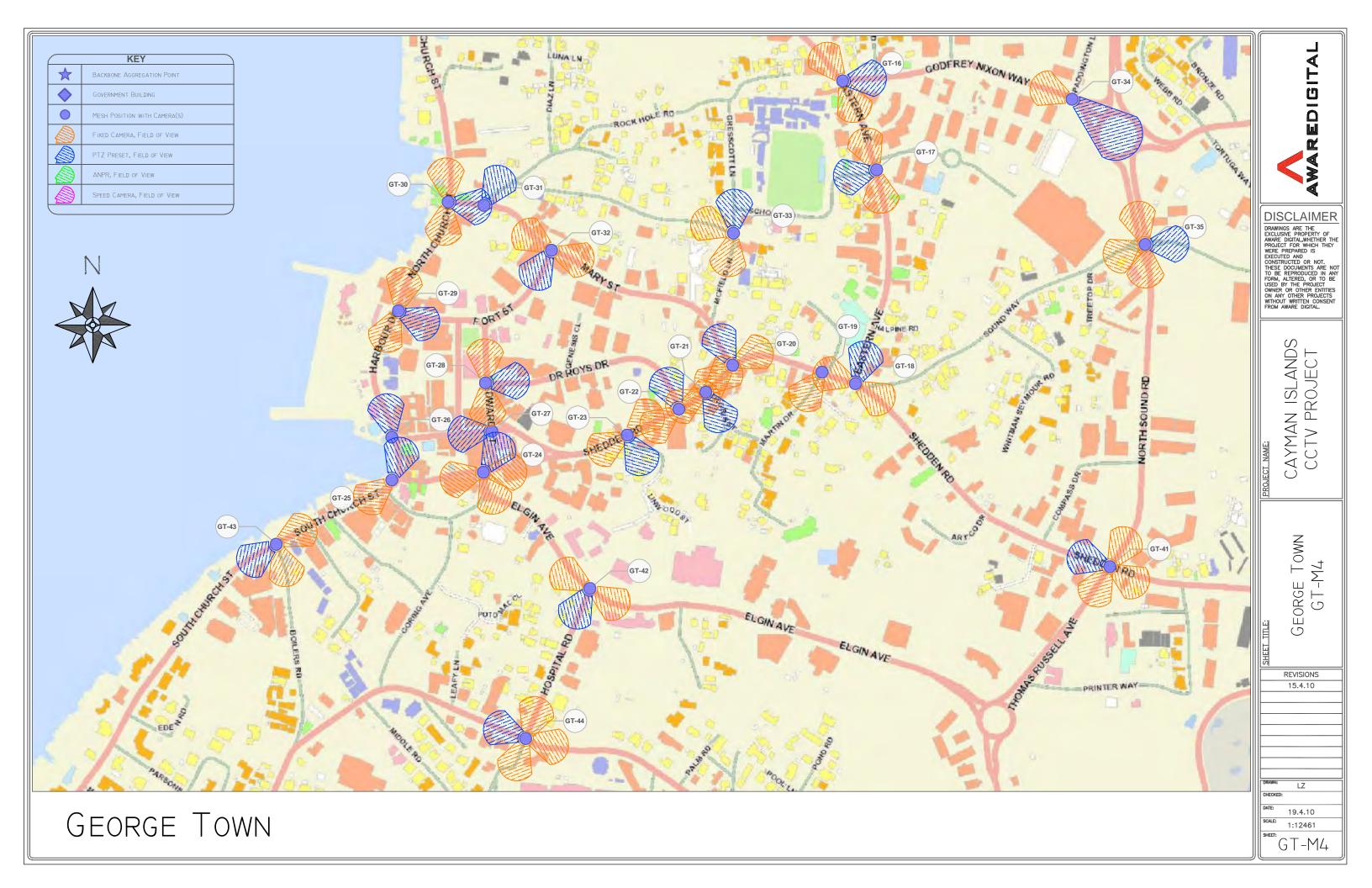




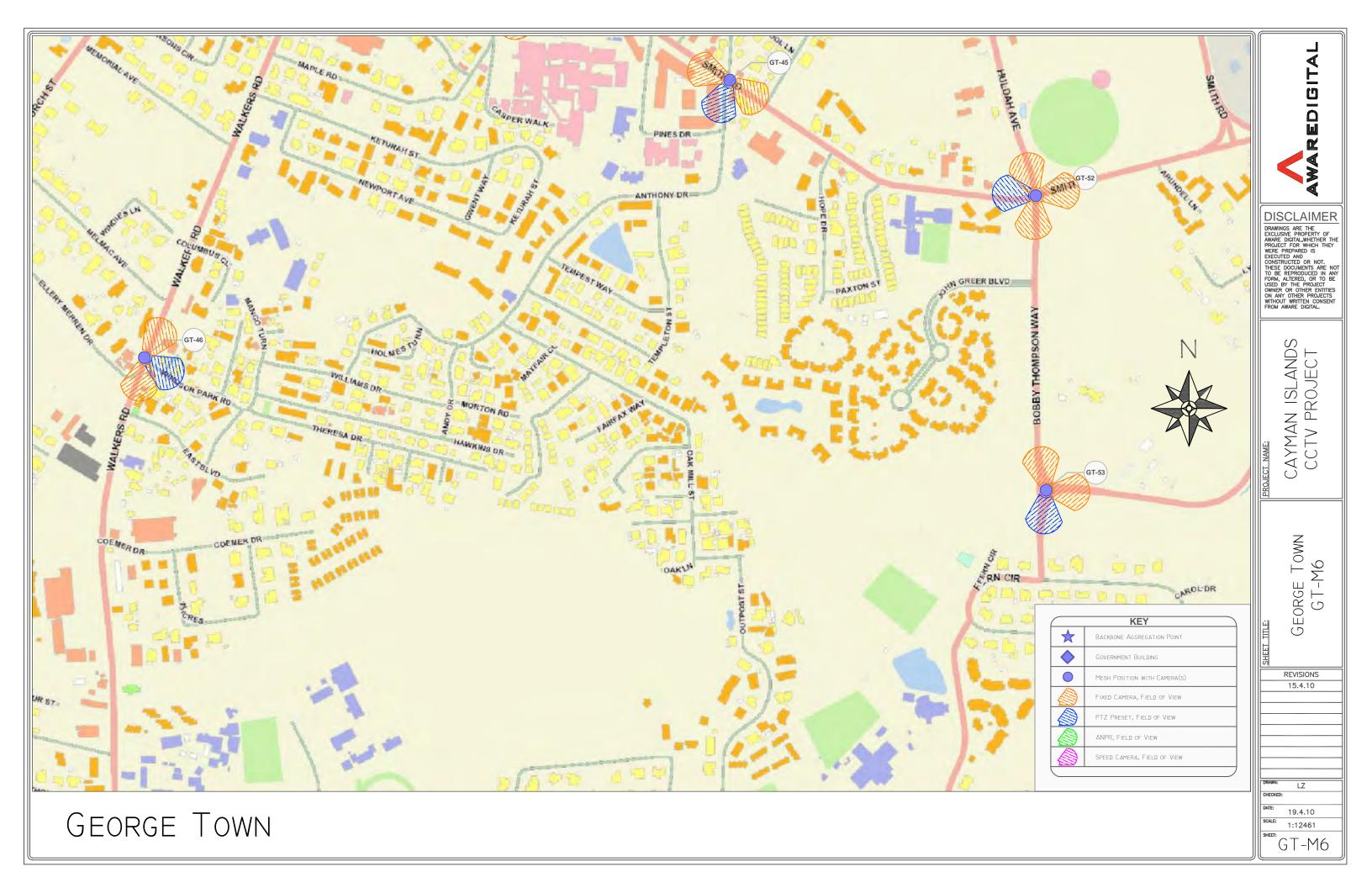


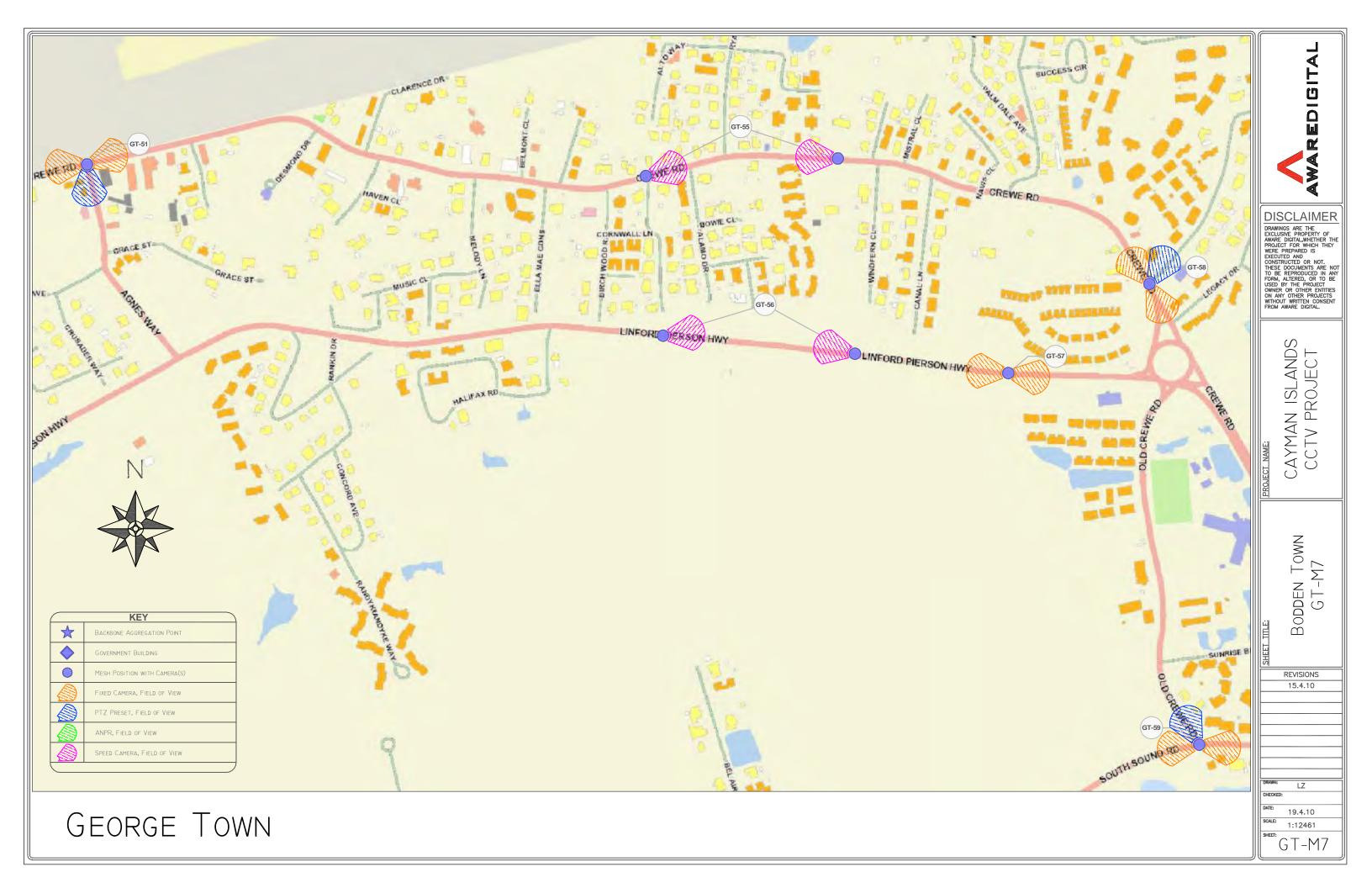


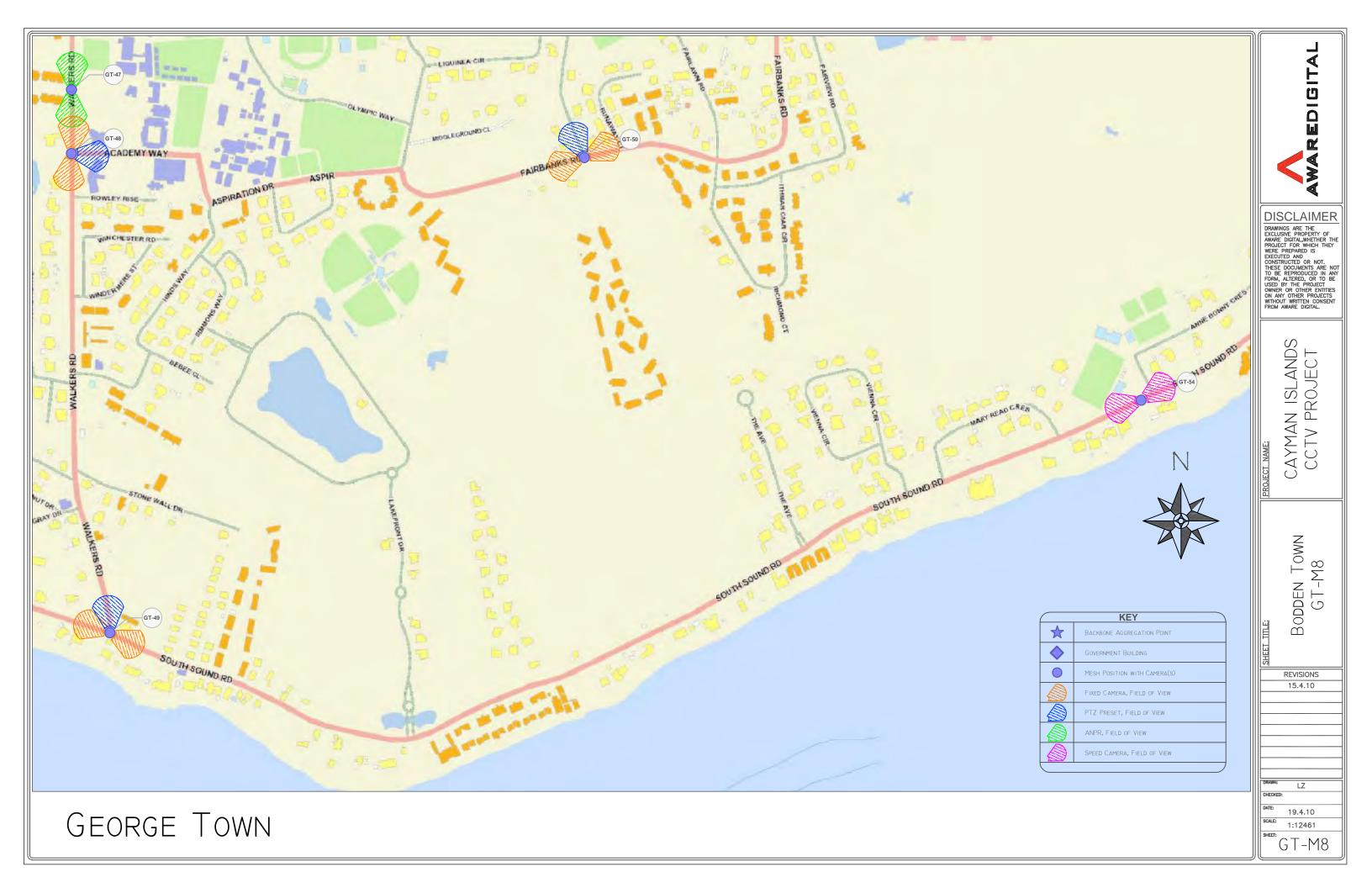
GT-M3

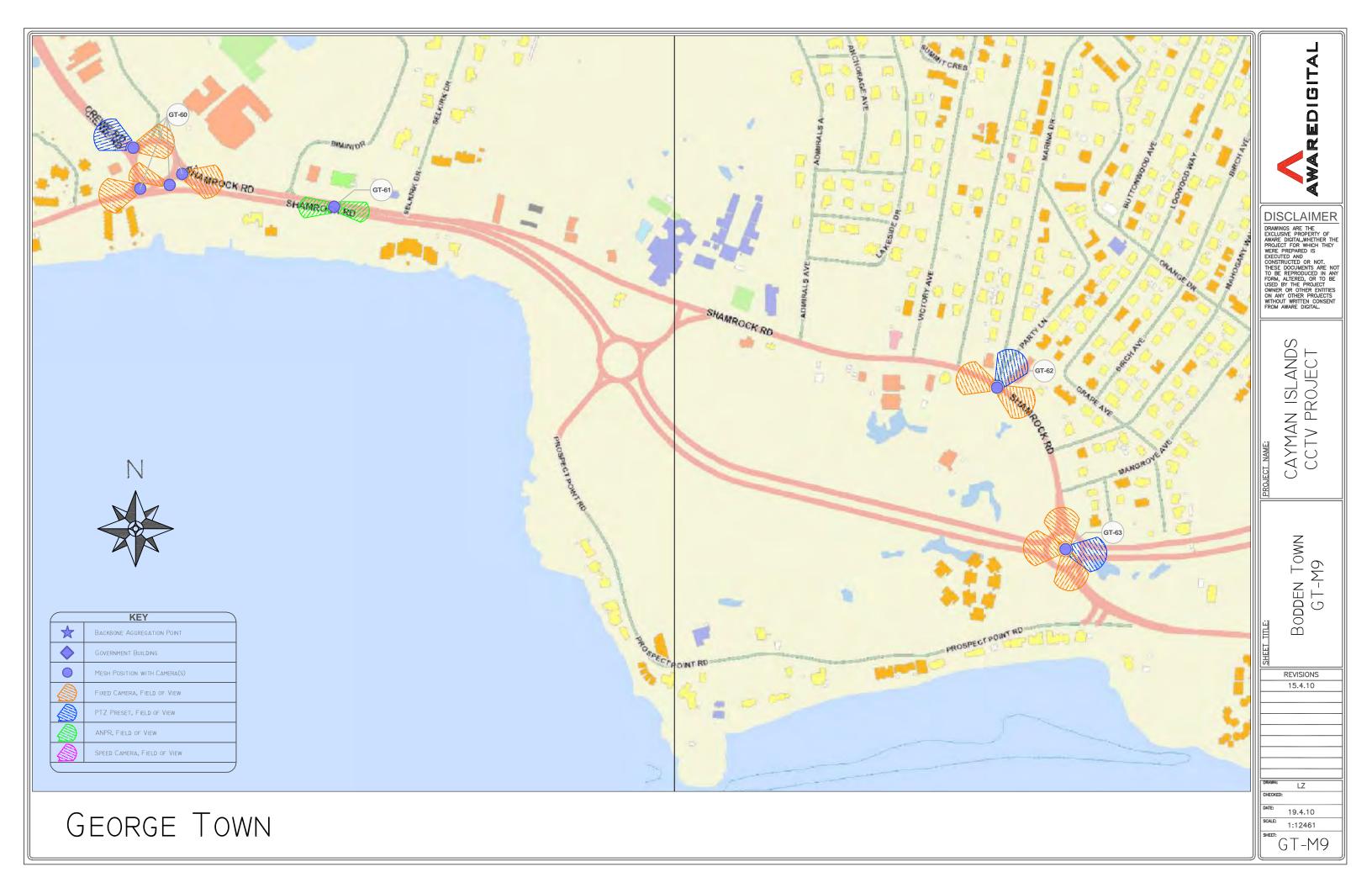




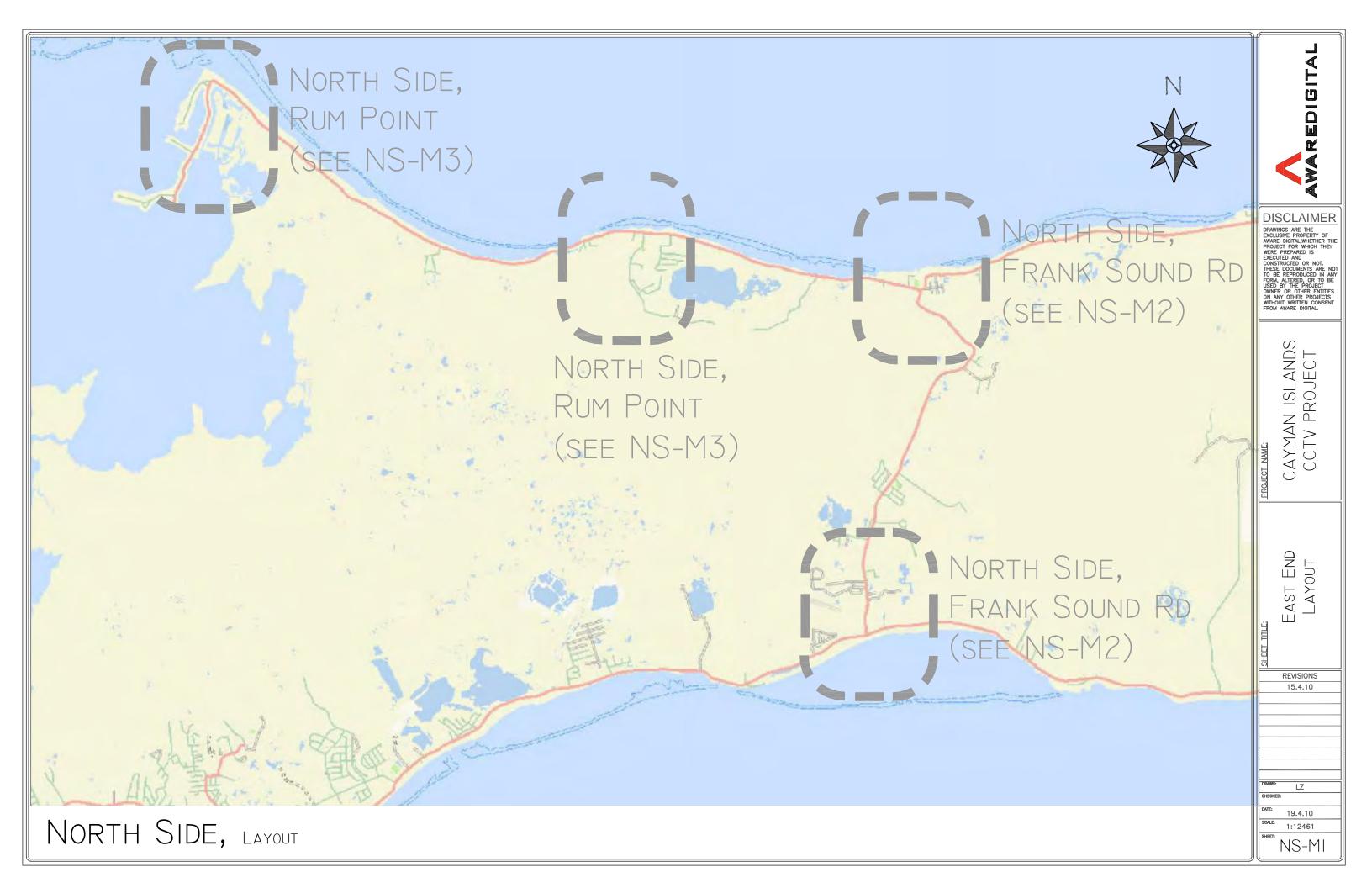


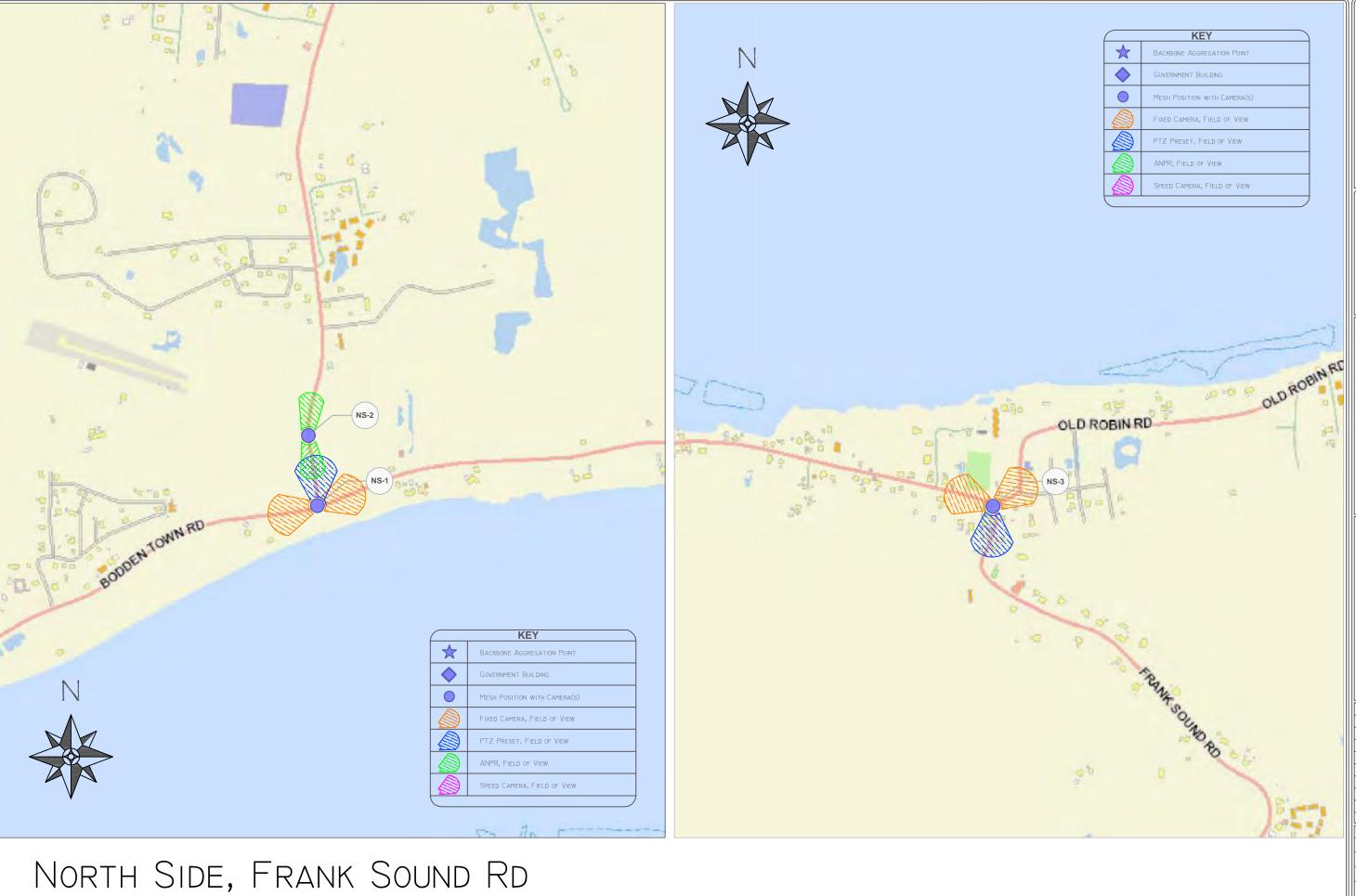












AWAREDIGITAL

DISCLAIMER

PRAWINGS ARE THE CXCLUSIVE PROPERTY OF WARE DIGITAL, WHETHER THE PROJECT FOR WHICH THEY WERE PREPARED IS XECUTED AND TO THE PROJECT OF THE PR

CAYMAN ISLANDS CCTV PROJECT

> NORTH SIDE FRANK SOUND RD

DEMISIONI

15.4.10

DRAWN:

19.4.10 ALE: 1:12461

NS-M2



