Pennsylvania Office of Open Records
333 Market Street, 16th Floor
Harrisburg, PA 17101-2234
openrecords@pa.gov

September 18, 2024

To the Attention of the Pennsylvania Office of Open Records:

On July 29, 2024, I filed a Right to Know request with the Beaver County ESU via letter sent to Right to Know Officer Detective Lt. Bonnie Sedlecak. **(EXHIBIT A)**

Detective Bonnie Sedlacek failed to respond timely and did not return multiple follow up phone calls or emails. No response at all was provided until a follow up call was placed to the District Attorney's Office on August 23, 2024. After an extensive call which included the warning that civil action would follow. Detective Sedlacek finally responded by email on August 26, 2024. **(EXHIBIT B)**

Neither the Beaver County District Attorney, nor Right to Know officer Detective Bonnie Sedlacek have denied any aspect of this request in whole or in part, but rather, they have simply failed to fulfill the request in contradiction to the written response.

The records sought are police photographs, videos and writing documentation created during or in the course of public police and other activities related to murder and attempted murder that took place during a political rally for presidential candidate Donald Trump in Butler, PA on July 13, 2024.

Pennsylvania Statutes Title 65 P.S. § 67.901 mandates that the time for response to a Right to Know request shall not exceed five business days from the date the written request is received by the open-records officer for an agency. Detective Sedlacek's response was not timely. Moreover, when the response did arrive it failed to adequately fulfill the request. A USB thumb drive was sent on August 30, 2024, **(EXHIBIT C)**

Pursuant to Pennsylvania's Right to Know Act, (65 P.S. § 67.102): A public record is defined as any information documenting a transaction or activity of an agency, created, received, or retained pursuant to law or in connection with a transaction, business, or activity of the agency. This applies regardless of the form the information takes (paper, email, recordings, etc.).

Exceptions to Public Records as defined in 65 P.S. § 67.708(b) may exclude such records that would threaten public safety, relate to criminal investigations, or include personal information like Social Security numbers.

In this case, ongoing efforts to assassinate presidential candidate Donald Trump, (https://www.nytimes.com/2024/09/15/us/politics/trump-shooting-golf-course.html) and the danger those efforts pose to the candidate and the public outweigh considerations of any ongoing investigation in Pennsylvania. Furthermore, in consideration of the fact that one member of the public was violently murdered and others suffered severe injuries at the Butler event, public interest weighs in favor of disclosing the records as requested.

No specific denial was issued upon the initial request. An apparent error on the part of Beaver County Right to Know Officer Detective Bonnie Sedlacek, has already made the content of the records in question public. Withholding original unaltered copies of the records will not serve to protect any legitimate ongoing investigation if one remains ongoing at this time.

The requested records do not meet the requirement of any of Right to Know exceptions and no exceptions have been cited by Beaver County. In a follow up telephone conversation on or around September 13, 2024, Chief Detective Patrick Young stated unequivocally, "we released everything to the congressional committee, in whatever the purest format that we had."

However, Detective Young's statement is undeniably false. In a separate police record included in the documents provided, a bodycam video designated "Recording 2024-08-23 Redacted MH0C0012.mp4" depicts Detective Richard Gianvito at timestamp 19:09:03, handling an iPhone that clearly shows the photographs in question on screen. Further, the unredacted documents provided indicate that the photos in question were taken by Detective Gianvito. This would mean the original copies of those photos should be stored on Detective Gianvito's phone and should have been preserved in their original format.

The July letter to Detective Sedlacek described in detail, technical and forensic issues observed in the evidence photos that indicate manipulation with Adobe Photoshop or other similar computer software. The photos are contained both in a Powerpoint document titled "FPOTUS After Action-redacted..pptx" and also as independent .jpg image files. Despite being designated as "redacted," the Powerpoint document contained unredacted photos and the names and phone numbers of officers involved in collecting and processing the photo data. According to these unredacted documents, the photo was sent by text message to an individual at the phone number [redacted]. The document states this was requested by "EOD" which is believed to be the Explosive Ordnance Disposal unit of the Philadelphia field office of the Alcohol Tobacco and Firearms Bureau. In a phone call with the alleged ATF agent, on or around September 13, 2024, the agent did not deny the allegation that the image had been altered.

The iPhone depicted in Detective Gianvito's hand in the bodycam video is visibly identifiable as a model 11 or newer. This would indicate a camera resolution of 4,032 × 3,024, but the photos as provided are dramatically lower resolution of 640x480. Additionally, a photo designated as "Facial Recognition Photo" shows significant signs of digital alteration.

As an initial matter, and according to the National Institute of Standards and Technology ("NIST") in order for a photograph to be suitable for facial recognition, it must meet the following requirements to ensure accuracy. Here are the key characteristics:

1. High Resolution

• The image should have a high resolution to ensure that facial features are clearly visible. This usually means a minimum of 500 x 500 pixels but preferably higher (e.g., 1000 x 1000 pixels or more). A higher resolution allows facial recognition software to capture finer details of the face, such as skin texture and subtle contours.

2. Frontal Face View

• The subject should face the camera directly, with their head centered and no extreme tilts or angles. A straight, frontal pose ensures that all facial features are in the expected positions for the recognition algorithm to process.

3. Even Lighting

• The face should be evenly lit with no harsh shadows or overexposure. Proper lighting avoids obscuring facial features and maintains uniformity in skin tone, allowing the software to detect features like eyes, nose, and mouth accurately.

4. Neutral Expression

• Ideally, the subject should maintain a neutral facial expression, typically with the mouth closed and eyes open. Smiling or other exaggerated expressions can distort facial features, making recognition more challenging.

5. Minimal Background Clutter

• A simple, plain background (often white or neutral-colored) is preferred to avoid distractions. Complex backgrounds may interfere with the software's ability to isolate the subject's face, which can reduce accuracy.

6. No Obstructions

• The face should be unobstructed, meaning no glasses (unless they are clear), hats, masks, or large jewelry. Facial recognition works best when the entire face, including the forehead, eyes, nose, and chin, is clearly visible.

7. Uniform Camera Quality

• The photograph should be taken with a camera of sufficient quality (preferably 10 megapixels or higher) to ensure clarity. Cameras with poor focus or noise can degrade image quality, which negatively impacts the software's ability to identify key points on the face.

8. Consistent Angle and Distance

• The photo should be taken at eye level and at a consistent distance (typically 0.5 to 1.5 meters) from the camera. This ensures that facial proportions remain correct, and the subject's face occupies a significant portion of the frame.

9. No Excessive Post-Processing

• Photos that have been heavily retouched or filtered (e.g., Instagram or Snapchat filters) are not ideal for facial recognition. The software relies on natural features, so altering the image through post-processing can hinder accurate analysis.

10. Color Balance

• Proper color balance ensures that the skin tone and other facial features are accurately represented. Color distortion, due to incorrect white balance or lighting, can confuse the recognition algorithm.

11. ISO and Sharpness

• A low ISO setting ensures that the image isn't grainy or noisy, and a sharp, in-focus image allows the software to detect features more precisely.

By following these guidelines, a photograph will be better suited for accurate and reliable facial recognition, whether for security, identification, or other applications.

Sources:

• NIST Guide for Facial Recognition Quality

• ISO/IEC 19794-5:2011 - Biometric Data Interchange Formats for Facial Recognition

The photograph presented as a "facial recognition" image in the RTK response meets none of these standards and simply cannot be described as a "facial recognition" photograph. **(EXHIBIT D)**

Page 19 of a Powerpoint document included in the response and designated as "FPOTUS After Action-redacted" contains four "DOA confirmation" photographs. Despite the title, the unredacted document reveals these photographs were also taken by Detective Richard Gianvito. Two of the photographs show the suspect's right ear. **(EXHIBIT E)**

The suspect's right ear is also prominently shown in the alleged "facial recognition" photo on page 40 of the same document, however distinctive differences are clearly visible. This difference, coupled with lighting anomalies in the photo give rise to strong suspicion of digital manipulation which alters the content of the photo. If these suspicions are correct, the implications of such editing are substantial and could amount to criminal evidence tampering.

Given each of these considerations, and especially due to the fact that negligence on the part of Beaver County Right to Know officers has already made the content of the photographs public, releasing the original full resolution images as recorded on detective Gianvito's iPhone could not have any impact on ongoing investigations. In fact, given the clearly articulated suspicions, the immediate release of the original unalerted photo would be in the interest of the Beaver County ESU and RTK officers because it would dispel any suspicion.

Apple iPhone cameras record photos in a proprietary format known as High Efficiency Image Container, ("HEIC"). It is this original .HEIC format that was initially sought and this is the file format sought again now by this Right to Know appeal.

This appeal seeks true and accurate digital copes each of the original files of DOA photos and the "facial recognition photo" in their original .HEIC format and full resolution as recorded on Detective Richard Gianvito's iPhone on July 13, 2024. There is no legitimate reason to withhold these files and given the high degree of national public attention on this matter and the suspicion raised by shortcomings in the existing disclosures, the release of these files is exceptionally important. Releasing the images serves the public interest and would protect public safety and is legally mandated pursuant to Pennsylvania's Right to Know Act. Thank you for your prompt attention to this matter.

Jason Goodman
[redacted]

**(EXHIBIT A)**

Detective Lt. Bonnie Sedlacek
Right to Know Officer
Beaver County Detective Bureau
810 Third Street
Beaver, PA 15009
Email: bsedlacek@beavercountypa.gov

July 29, 2024

Dear Detective Lt. Sedlacek,

Thank you for speaking with me just now. I am writing in regard to the photograph we discussed apparently taken by a member of the Beaver County ESU SWAT team on the roof of American Glass Research on July 13, 2024. The photo is of a deceased suspect, reported to be Thomas Crooks but suspected to be Maxwell Yearick.

The photo in question is alleged to have been taken by a SWAT officer with his personal or department issued mobile phone camera which appears to be an Apple iPhone, unknown model. A SWAT officer recorded on the bodycam footage released to Senator Chuck Grassley can be seen scrolling through the phone and the picture in question, in addition to other similar pictures likely taken at the same time, can be clearly seen very small on the screen of the officer's phone.

This Right to Know Request concerns the original photographs and metadata related to those photographs as recorded on the officer's phone. I am a former cinematographer and stereoscopic visual effects expert with thirty-nine years of traditional and digital photo manipulation expertise.

I have evaluated a version of the photo allegedly taken by this Beaver County ESU SWAT officer and "leaked" to the internet on or around July 14, 2024. My expertise tells me that the leaked photo has been manipulated. The image of the deceased suspect's ear exhibits artifacts and other anomalies that suggest it may have been digitally altered.

Although it is difficult to discern the actual iPhone model being held by the officer in the bodycam footage, its overall shape indicates it is at least an iPhone 10, released in 2017. Even if the officer used the lowest resolution settings, I would expect an image of at least 2048x1536 resolution. The leaked photo was 1200x901. The "901" dimension is extremely odd and is a completely non-standard resolution.

I suspect this resulted from an inexperienced Photoshop user cropping a larger image with the crop tool set to inches rather than pixels. When a very high-resolution image is cropped and inches are prioritized, pixels are mathematically averaged to achieve the proper size. If the pixel height of a photograph cropped to 4:3 aspect ratio is not divisible by three, an odd numbered resolution will occur just like this. I observe and correct for that odd/even issue daily.

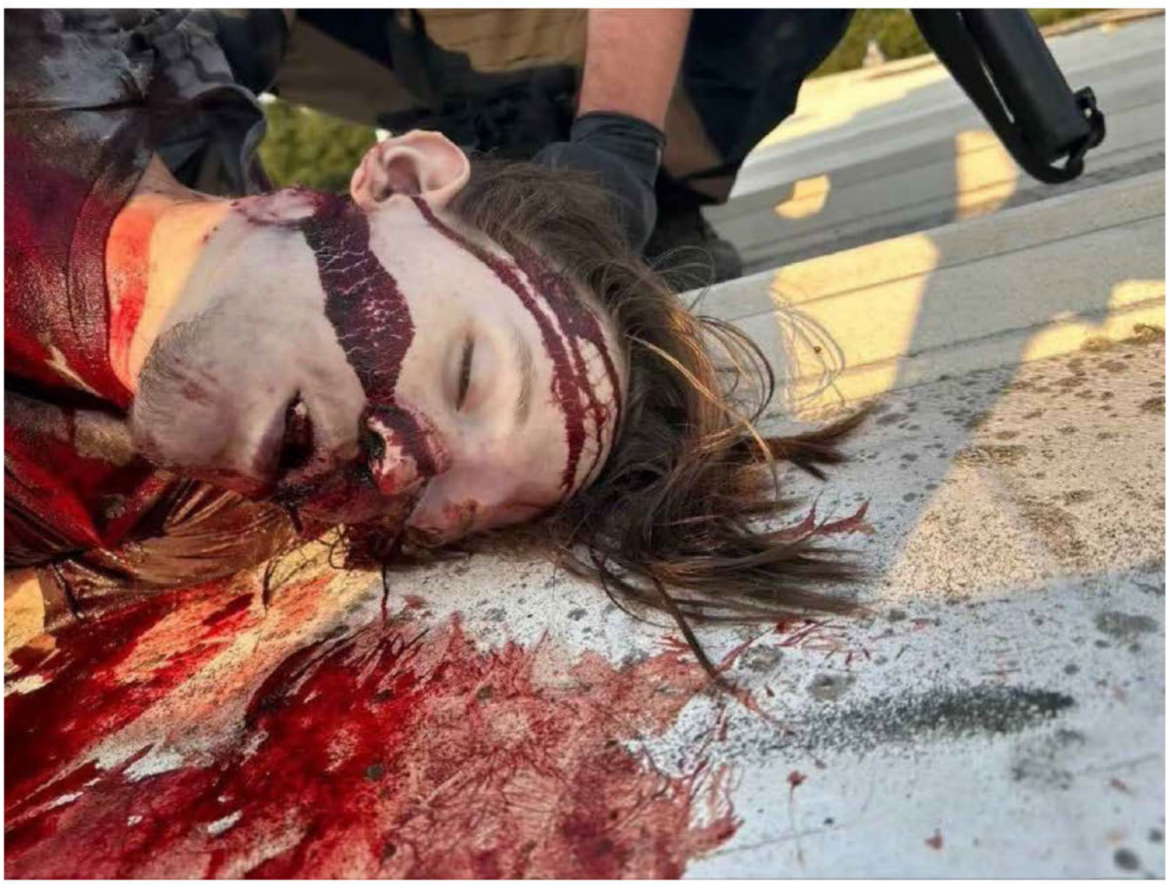
Additionally, heavy JPEG artifacts can be seen in the leaked photo, far greater than what would be present in a photo taken directly out of the phone. Issuing a heavily compressed "leaked" photo replete with JPEG artifacts would reduce an expert's ability to do proper forensic analysis of the image and would hide many errors often introduced in photo retouching. This final step is almost like adding a layer of dirt on top of a printed paper photograph.

Lastly, one accidentally unredacted frame in the Bodycam footage released to Chuck Grassley's office reveals the dead suspect's ear and although the bodycam extracted screen capture is somewhat low resolution, the suspect's ear does **NOT** appear to match the very distinctively shaped ear in the leaked photo. The allegedly retouched ear shown in the leaked photo matches the distinct ear shape seen in some photos of the known subject, Thomas Matthew Crooks.

Please provide any and all photographs including body camera video, and any photos or videos recorded on privately owned or department issued mobile phones or other recording devices from all Beaver County SWAT ESU members taken on July 13, 2024 and relevant to the assassination attempt against former U.S. President Donald Trump or related activity in or around American Glass Research 603 Evans City Rd, Butler, PA 16001.

If you require any additional information from me to fulfill this request or for any other purpose, please feel free to contact me. Thank you for your assistance in this matter.

Jason Goodman
[redacted]



*1200x901 jpeg photographed leaked to the internet shortly after July 13, 2024*

**(EXHIBIT B)**

**From:** **Bonnie Sedlacek** BSedlacek@beavercountypa.gov
**Subject:** RE: Right to Know Request re: American Glass Research July 13 body cam cell phone and other photo/video evidence
**Date:** August 26, 2024 at 1:05 PM
**To:** Jason Goodman [redacted]

---

Good Morning,

The requested records are approved. Please see attachment.

Lieutenant Det. Bonnie L. Sedlacek" Drug Task Force Supervisor
Beaver County District Attorney" Detective Bureau
810 Third Street" Beaver, PA 15009
Phone:724-773-8576" Fax:724-728-5249
Cell:724-624-1527
www.beavercountypa.gov" bsedlacek@beavercountypa.gov



-----Original Message-----
From: Jason Goodman <[redacted]>
Sent: Monday, July 29, 2024 10:59 AM
To: Bonnie Sedlacek <BSedlacek@beavercountypa.gov>
Subject: Right to Know Request re: American Glass Research July 13 body cam cell phone and other photo/video evidence



Thank you for speaking with me earlier detective. Please let me know if any additional information is required.

Jason Goodman
[redacted]

**RTK-Act 22 Invoice Trump Rally 2024.pdf**
42 KB

Nathan L. Bible
DISTRICT ATTORNEY

Tina Price-Genes
EXECUTIVE ADMINISTRATIVE
ASSISTANT

BEAVER COUNTY

DISTRICT ATTORNEY'S OFFICE

COURTHOUSE
810 THIRD STREET
BEAVER, PENNSYLVANIA 15009

724-773-8550
Fax: 724-728-0710

Patrick Young
CHIEF COUNTY DETECTIVE

Brittany Smith
FIRST ASSISTANT DISTRICT
ATTORNEY

**Invoice**

26 August 2024

**RE: Right to Know Request/Act 22 of 2017 Received for Trump Rally 14 July 2024 records.**

Records: Please indicate **X** chosen option.

( )1 8gb SanDisk Flashdrive - $4.99
Or
( ) 1 Verbatim 4.7 GB DVD+R - $1.00

Mailing/Shipping costs- $1.50

*costs of this invoice will need to be satisfied prior to the release of data.

Please make Checks Payable to: Beaver County District Attorney
Attn: Open Records Officer/ Detective Lt.Bonnie Sedlacek
810 Third Street
Beaver, PA 15009

Any questions please contact Detective Lt. Bonnie Sedlacek, Open Records Officer.
724-773-8576.

**(EXHIBIT C)**

Beaver County District Attorney's Office
810 3rd
Beaver,

PITTSBURGH P&DC 152
FRI 30 AUG 2024 PM

Jason Goodman
[redacted]

**(EXHIBIT D)**

# Face Recognition Vendor Test Ongoing

# Face Recognition Quality Assessment

## Concept and Goals

VERSION 1.0

Patrick Grother
Mei Ngan
Kayee Hanaoka
*Information Access Division*
*Information Technology Laboratory*

Contact via frvt@nist.gov

April 23, 2019

National Institute of Standards and Technology
U.S. Department of Commerce

## 1. Scope

While standards exist for interchange of face images [ISOIEC-2005 superseded by ISOIEC-2019 which includes , ICAO-Portrait, and ANSI-NIST Type 10] and those standards additionally regulate the capture of images, there are no standards for how face image quality must be assessed[1] nor are there performance evaluations for automated quality assessment algorithms.

This document is intended to support accurate face recognition by:

- Establishing specifications for face image quality assessment algorithms that return scalar quality values, particularly by requiring image quality assessment algorithms to judge quality in reference to ISO/IEC 19794-5 full frontal and the ICAO Portrait Quality standards;
- Describing NIST's performance evaluation of such algorithms.

## 2. Applications of quality scalars

The primary use cases for scalar image quality assessments are:

- **Photo acceptance**: Foremost, scalar image quality values can be used to make an acceptance or rejection decisions. If an image's quality is too low, a system will reject the image and initiate collection of a new image. Such a process could be implemented in a camera, in a client computer, or on a remote server. Such a capability is most useful during initial enrollment, when a prior reference image of the subject is not available. It is also useful when forwarding the image to a remote recognition service would be time consuming or expensive.
- **Quality summarization**: Scalar image quality values are useful as a management indicator. That is, in some enterprise where face images are being collected from many subjects, say by different staff, at different sites, under different conditions, the quality values can be used to summarize the effectiveness of the collection. This might be done using some statistic such as average quality, or proportion with low quality. Such summarization can be used to reveal site-specific problems, population effects, as a response variable in A-B tests, and to reveal trends, diurnal or seasonal variation.
- **Photo selection:** Given K > 1 images of a person, select the best image. This operation is useful when a receiving system expects exactly one image, and the capture subsystem must determine which of the several collected images should be transmitted. This application of quality is useful when a capture process includes some variation e.g. due to unavoidable motion of the subject or camera.

  NOTE Ordinarily this function should not be used in place of recognition. A recognition application should generally enroll all K images of a person rather than select one. This recommendation is made because quality assessment infrastructure is an imperfect predictor of recognition outcome and it may arise that an enrolled image with lower quality might be successfully matched to a probe image due to certain characteristics of the image e.g. view angle or facial expression. That said, if some images may have been collected decades ago, then ageing may well reduce the utility of the image to a recognition against a recent image even if quality is excellent.

[1] The document ISO/IEC 29794-5:2010 is a technical report that, as such, does not establish any requirements that a formal standard would do. Its title is "ISO/IEC 29794 Biometric sample quality — Part 5: Face image data". It gives terminology, base concepts, and examples of how specific quality degradations might be measured.

# 3. Quality Assessment

## 3.1. Prior standardization

Table 1 in technical report ISO/IEC 29794-5:2010 characterizes two aspects of face quality. The first distinguishes between subject-specific factors, and environmental and capture system factors. The second decomposes persistent "static" effects from those that occur temporarily. Table 1 is an excerpt of the table in the ISO document expressing that quality problems due to mis-presentation by the subject and those related to imaging are in many cases separable – for example photographs can be systematically mis-focused even when the subjects present perfectly.

*Table 1 – Characterization of Face Image Quality*

| | Subject characteristics | Acquisition process |
|---|---|---|
| Static properties | Biological characteristics:<br>– injuries and scars<br>– ...<br>Other static characteristics<br>– Thick or dark glasses<br>– Permanent jewellery | Acquisition process and capture device properties:<br>– image resolution<br>– optical distortions<br>– ...<br>Static properties of the background<br>– [textured] wallpaper |
| Dynamic properties | Subject characteristics and behavior:<br>– exaggerated expression<br>– hair across the eye<br>– ... | Scenery<br>– background moving objects<br>– variation in lightning<br>Capture device variation<br>– mis-focus<br>– poor exposure (due to bright sources) |

Note that in traditional live-scan fingerprint capture, quality problems related to imaging are essentially absent by virtue of the optical design and mode of operation of the sensor. For this reason, it was possible to build fingerprint quality assessment algorithms [NFIQ] that did not need to quantify quantities such as illumination non-uniformity and mis-focus. For face recognition, however, the distinctions inherent in the table influence what quality measurements should be made, as discussed next.

## 3.2. Fundamental operations

### 3.2.1. Scalar quality value

Given an image X, an image quality assessment algorithm, F, shall produce a scalar quality score, Q = F(X). Four examples are shown in Figure 1. The progression, from left to right, implies that better images have higher quality values, where the term better here is the subject of this standard.

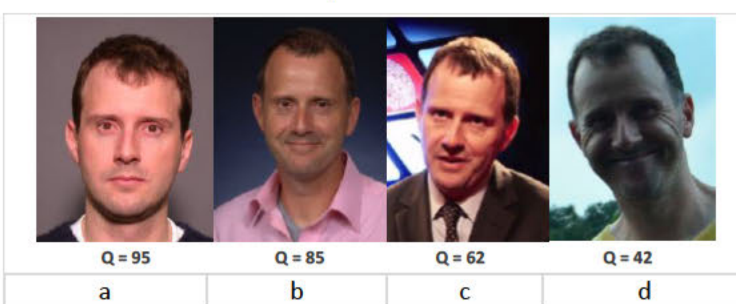


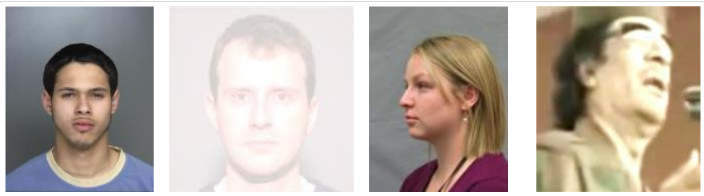

*Figure 1 –Four faces with example image quality values.*

### 3.2.2. Quality 2-tuples

**NOTE Reporting of quality tuples is not part of the FRVT Quality Evaluation in 2019.**

Given image X, a quality assessment algorithm, F, shall report $(Q_{SUB}, Q_{SYS}) = F(X)$ where the scalar $Q_{SUB}$ reflects subject-specific behavior, and $Q_{SYS}$ summarizes properties inherent in the environment and imaging system.

- $Q_{SYS}$ should summarize quantities like resolution, compression, illumination amount, non-uniformity and sensor noise i.e. items which would be expected to affect all images collected from that system.
- $Q_{SUB}$ should summarize quantities like expression neutrality, pose, eye openness and eyeglasses.



| | | | |
|---|---|---|---|
| $Q_{SUB} = 98$<br>$Q_{SYS} = 90$ | $Q_{SUB} = 94$<br>$Q_{SYS} = 40$ | $Q_{SUB} = 20$<br>$Q_{SYS} = 95$ | $Q_{SUB} = 28$<br>$Q_{SYS} = 23$ |
| a | b | c | d |

*Figure 2 - Four faces with example quality 2-tuples*

Figure 2b shows an image in which the subject presents almost perfectly to the camera, but photo quality is impaired by poor exposure. In contrast, Figure 2c shows an image in which the imaging is good, but the subject mis-presents to the camera. Figure 2d shows an image with both kinds of problem, and Figure 2a has neither.

## 3.3. Quantitative goal for quality scalars

ISO/IEC 29794-1 delineates three aspects of the umbrella term quality:

- *Character:* This is some statement of the normality of the anatomical biometric characteristic – thus a scarred fingerprint or a heavily bearded face may have poor character.
- *Fidelity*: This is any measurement that indicates how well a captured digital image faithfully represents the analog source – thus a blurred image of a face omits detail and has low fidelity.
- *Utility*: Finally, and most relevant in this standard, the term *utility* is used to indicate the value of an image to a receiving recognition algorithm.

This standard conceives of quality scalars as being measures of utility rather than, say, fidelity, because utility of a sample to a recognition engine is what drives outcome operationally and is of most interest to end-users[2].

The standard, later, requires quality values to serve as predictors of true match outcome. Of course, recognition outcomes depend on the properties of at least two images, not just the sample being submitted to a quality algorithm. This apparent disconnect is handled by requiring sample quality to reflect expected comparison outcome of the target image with a canonical high-quality portrait image of the form given in Figure 3.

[2] The adoption of utility provides a quantitative goal for development of quality scalars, in the supervised machine learning sense. This approach was taken with the NIST Fingerprint Image Quality Algorithm. The ISO/IEC 29794-4 standard defines the NFIQ algorithm which was trained using a machine learning scheme to be a predictor of fingerprint true match accuracy. That algorithm, and its commercial analogues, have been run tens of billions of times in large scale identity operations in many global programs, including Aadhaar (India) and immigration (USA).

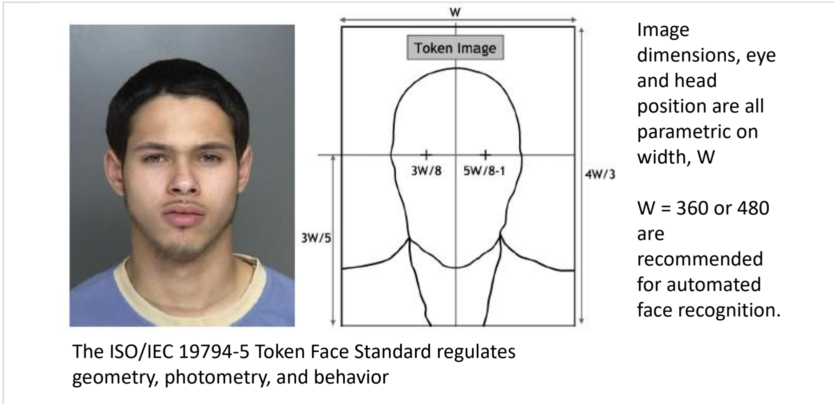



*Figure 3 – Canonical Portrait Photograph, as standardized in ISO/IEC 19794-5*

Formally, if a face verification algorithm, V, compares two samples $X_1$ and $X_2$, to produce a comparison score

$$S = V(X_1, X_2) \tag{1}$$

this standard requires quality algorithms to predict S from $X_1$ alone but under the assumption that $X_2$ would be a canonical portrait image i.e. a pristine image of the same subject that is fully conformant to ISO and ICAO specifications[3]. Thus, a quality algorithm F operating on an image $X_1$ produces value

$$Q = F(X_1) \tag{2}$$

that in the sense defined later predicts S because it implicitly assumes the comparison

$$V(X_1, X_{PORTRAIT}) \tag{3}$$

This goal respects the ISO/ICAO specification as the reference standard for automated face recognition. The light grey text indicates that quality assessment must be done blind[4], targeting a hidden virtual portrait image.

Without this formulation of the quality problem the position, noted in the academic literature, that quality assessment cannot be done on a single image - that quality should "come in pairs" - would be correct. Such assertions note that recognition outcomes (that are the result of comparing two images) depend on the properties of both images. For example, consider Figure 4. It presents the false non-match rates (FNMR) from three face verification algorithms executed on a database of images where facial pose (yaw) differs between the two images used in a comparison. Figure 4a corresponds to an algorithm that gives high FNMR except when the two images are frontal.

[3] A reasonable question here would be why the target must be a portrait. The answer is that it doesn't have to be, that quality assessment might be done also referencing some other standard view of a face. This might in fact be desirable once we recall that forensic face examiners have preferred views where the ear is visible. Indeed, the immigration agencies in the United States used to require a quarter-left view on identity document for just this reason. For now, however, the target must be the ISO/ICAO portrait because the face recognition industry is currently capitalized on the basis of frontal face recognition. This standard could be extended to adopt quality assessment against some other standardized view.

[4] The term "blind" is borrowed from the image fidelity literature in which a "blind PSNR" i.e. peak signal to noise ratio is computed from, for example, a JPEG image or a video clip as a statement of quality. Such techniques may have applicability here.

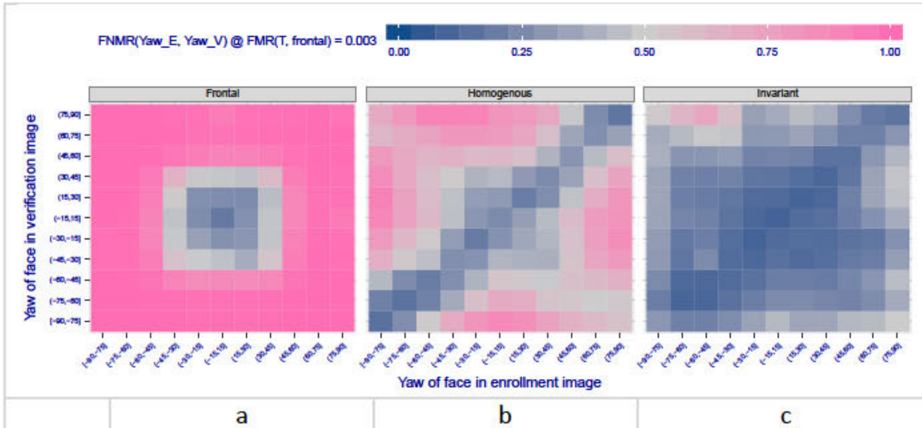



*Figure 4 – The classes of algorithm response to comparison of pairs of images that differ in the yaw angle of the face.*

This is the common case. Figure 4b shows an algorithm that is capable of matching images of a face with the same yaw angle, even if non-frontal. Finally, Figure 4c represents the (rare) case of an algorithm that offers considerable pose invariance[5].

The point of this example is that recognition outcome may actually depend on the pair of images, but quality assessment, run on a single image potentially long before any recognition occurs, must assume a reference standard, here the ISO/ICAO portrait.

## 3.4. Quality value as predictor of true matching performance

Quality values are most useful as predictors of false negative outcomes, arising from low genuine scores. The alternative, as predictors of false positives, is considered less feasible because these arise from high impostor scores which should result only from facial (e.g. anatomical) similarity of the input image pair. However, some recognition algorithms do yield spurious high impostor scores from certain images. Examples are from similar eye-glasses, or hair styles. Such effects are unwelcome but are not relevant to a quality standard.

## 3.5. Recognition algorithm dependence

This standard requires quality algorithms to predict false negative recognition outcomes. Of course, recognition algorithms extract various proprietary features from face images and have different accuracies and tolerance of quality problems. However, given extreme degradations they all fail: Sufficiently over- or under-exposed images will cause false negatives; blurred faces, likewise; faces presented at high pitch or yaw angles will generally cause failure[6]. The approach in building a quality algorithm, and in testing it, is to predict failure from a set of recognition algorithms.

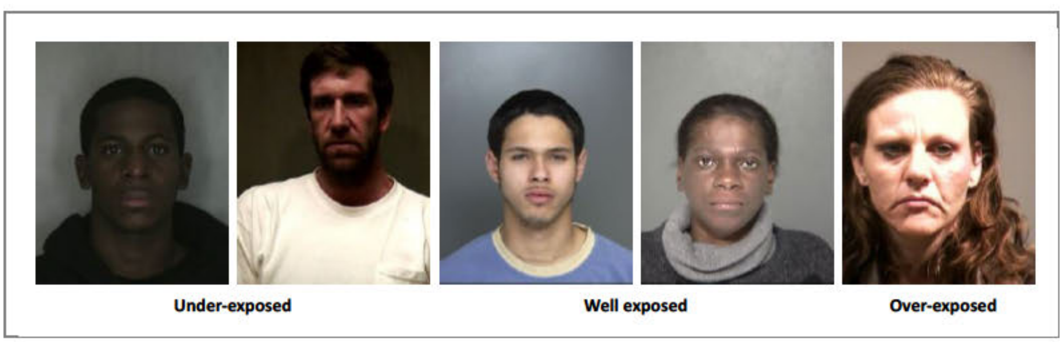



*Figure 5 – High-resolution non-frontal views for forensics*

[5] The figure is extracted from P. Grother, M. Ngan, K Hanaoka, *Ongoing Face Recognition Vendor Test (FRVT) Part 1: Verification*, NIST Interagency Report, 2019.

[6] The algorithm in Figure 3C shows wide pose invariance. However, this is a result for a recent (2018) prototype from a single developer, and frontal pose gives higher genuine scores even for this recognition algorithm.

# 4. Evaluation of image quality assessment algorithms

## 4.1. Overview

This section describes evaluation of algorithm submitted to NIST FRVT Image Quality Assessment Evaluation.

The evaluation is based on the execution of each quality assessment algorithm on large numbers of images for which reference target quality values are available.

## 4.2. Image and reference quality datasets

NIST will use several sets of images, initially reference portrait images. See NIST Interagency Report 8238 for recognition results using mugshot images.

For each image, NIST will establish reference quality values based on genuine recognition similarity scores obtained using that image. This assigns the lowest target scores to those images that are involved in false non-match errors. The annotation procedure might be based on an image quality oracle [Phillips13]. The target scores form the ideal performance of quality measures for a given data set.

NOTE Ageing causes face appearance to change and this causes genuine similarity scores to decline. This will occur even if all the images are perfectly captured with high quality. For this reason, the image quality assessment datasets will exclude image pairs for which there is large elapsed time between captures.

## 4.3. Performance metrics

The quality values should be predictors of the target scores. That is, the ordering of the quality values should be identical to that of the target scores, as required by [Grother07]. In general, this prediction will be imperfect, as shown in Figure 6.

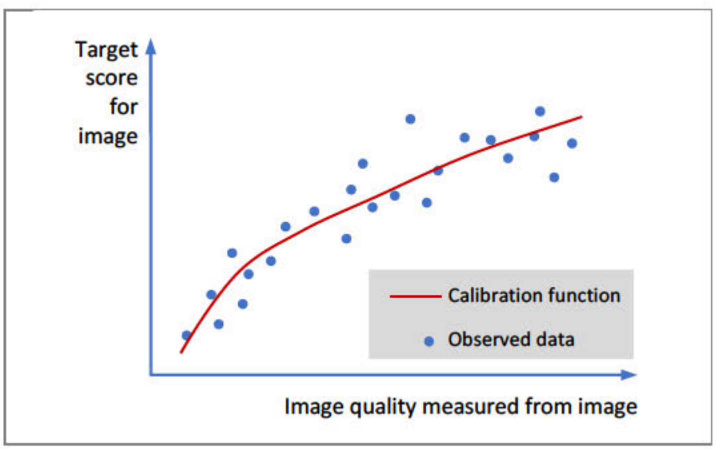



*Figure 6 – Example association of quality scores with targets*

Given N genuine image pairs, $x_i$, and N reference recognition scores, $t_i$, NIST will execute each image quality assessment algorithm to produce 2N quality values, $q_{1i}$ and $q_{2i}$ from which NIST will compute N values $q_i = \min(q_{1i}, q_{2i})$ . The use of min() embeds the assumption that a low comparison score will be caused by the image with the lower image quality.

NIST will relate quality to reference recognition scores several methods such as:

- Scalar measures of association, such as Kendall's correlation coefficient, particularly at low ranks.
- Error vs. reject plots [Grother07] computed by taking proportions of the lowest computed quality values and graphing[7] how closely they correspond to the lowest target scores.

[7] Specifically, when a proportion $0 < r \leq 1$ of the lowest quality values i.e. the set $Q = \{ i : 1 \leq i \leq L,\ q_i \leq q_{rN} \}$ are rejected this should lead to rejection of the lowest associated target values i.e. those that cause false rejections. Formally, compute

$$E(r) = 1 - L^{-1} \Sigma_Q H(t_i - T)$$

where T is the rN-th lowest target score; H is the unit step function; $t_i$, is the i-th target value; and index i runs over the rN indices in the set Q.

### 4.3.1. Handling failure to process

Given an IQAA, NIST will execute the image quality assessment algorithm on all 2N images in the reference dataset. This will generally produce $M \leq 2N$ quality values, $q_i$. We will assign $q_i = 0$ to the M failure cases.

The test report will disclose the number of failures, 2N – M.

### 4.3.2. Calibration

While quality values must exist on the range [0,100], their distribution within that range will vary between algorithms. For example, one IQAA might give most values on [60,100] while another might assign values on [10,90]. This implies a need to do calibration.

NIST will explore calibration by computing, for example, the function, shown in red in Figure 6, that results from isotonic regression [Han12] of target score against quality score. That function, F, minimizes $\Sigma(t_i - F(q_i))^2$ while requiring F to be monotonic. This can be achieved via the Pool Adjacent Violators algorithm. Once this function is available it can be used to map raw quality measurements, Q, to a calibrated quality F(Q) by simple lookup. F will generally not be linear.

NIST will report calibration functions.

## Bibliography

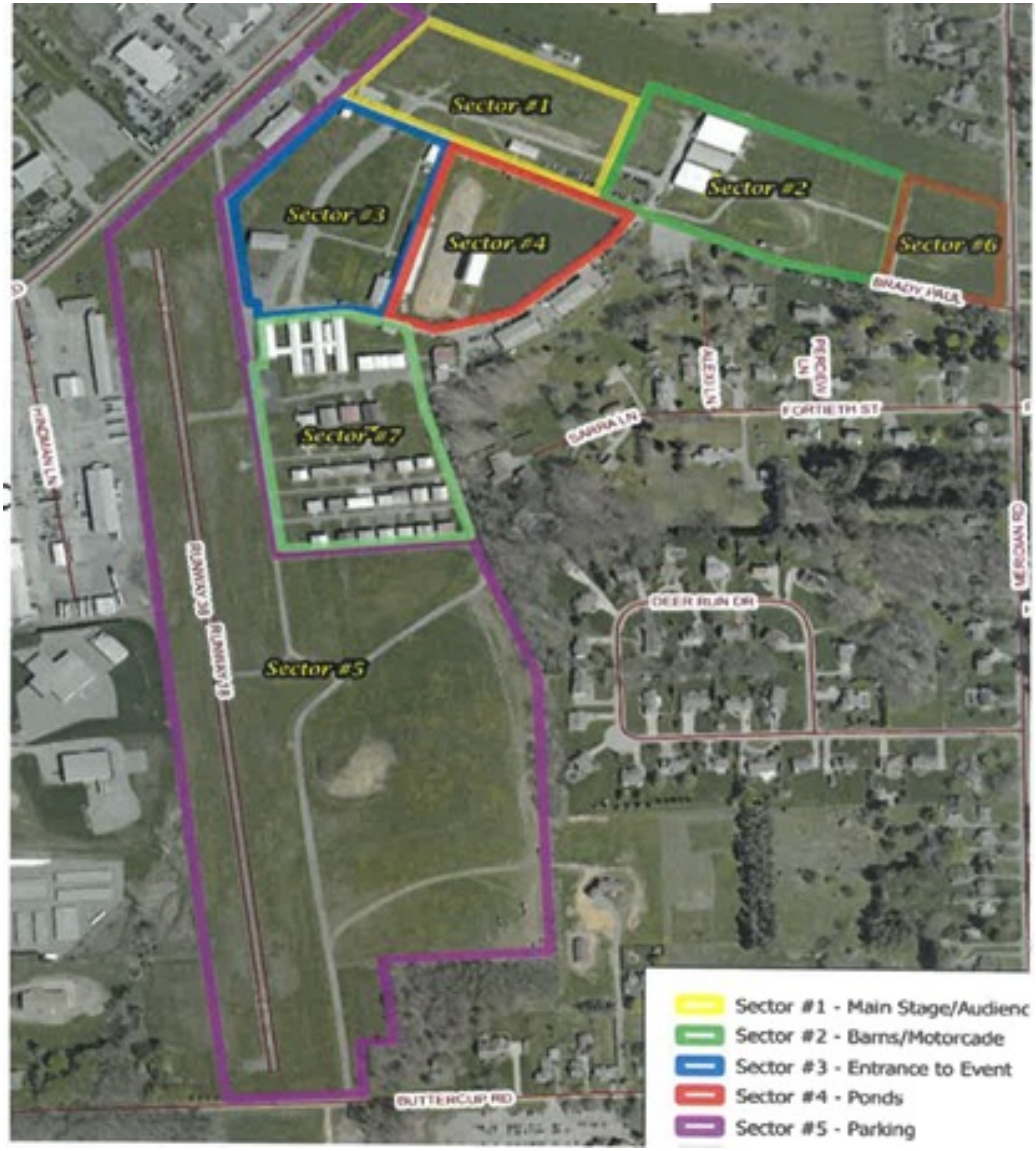

| | | |
|---|---|---|
| 1. | [Grother07] | Patrick Grother, Elham Tabassi, *Performance of Biometric Quality Measures*, IEEE Transactions on Pattern Analysis and Machine Intelligence, Volume 29, Issue 4, April 2007. https://ieeexplore.ieee.org/document/4107559/ |
| 2. | [Han12] | Yu Han, Yunze Cai, Yin Cao, and Xiaoming Xu, *Monotonic Regression: A New Way for Correlating Subjective and Objective Ratings in Image Quality Research*, IEEE Transactions on Image Processing, Volume: 21, Issue: 4, April 2012, Page(s): 2309 – 2313, 06 October 2011, DOI: 10.1109/TIP.2011.2170697 |
| 3. | [Phillips13] | P. J. Phillips, J. R. Beveridge, D. Bolme, B. A. Draper, G. H. Givens, Y. M. Lui, S. L. Cheng, M. N. Teli, and H. Zhang, *On the Existence of Face Quality Measures*, In proc. IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS 2013), September 30, 2013. http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=914258 |
| 4. | [ANSI-NIST Type 10] | NIST Special Publication 500-290 Edition 3, *Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information,* ANSI/NIST-ITL 1-2011, August 22, 2016 https://dx.doi.org/10.6028/NIST.SP.500-290e3 |
| 5. | [ISOIEC-2005] | ISO/IEC 19794-5:2005 Biometric Data Interchange Formats – Face Image data |
| 6. | [ISOIEC-2019] | ISO/IEC 39794-5:2019 Extensible biometric data interchange formats – Face Image data |
| 7. | [ISO-Geometry] | ISO/IEC 1974-5:2005/AMD 1:2007 Conditions for taking photographs for face image data |
| 8. | [ISO-Quality] | ISO/IEC TR 29794-5 Biometric sample quality -- Part 5: Face image data<br>Technical report for aspects of quality specific to facial images. It<br>– specifies terms and definitions that are useful in the specification, use and testing of face image quality metrics;<br>– defines the purpose, intent, and interpretation of face image quality scores.<br>Performance assessment of quality algorithms and standardization of quality algorithms are outside the scope of ISO/IEC TR 29794-5:2010. |
| 9. | [ISO-Conform] | ISO/IEC 29109-5:2014 Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 -- Part 5: Face image data.<br>This specifies conformance tests for the syntax of records defined in the ISO/IEC 19794-5:2005 biometric data interchange format standard. |
| 10. | [ICAO-Portrait] | PORTRAIT QUALITY - REFERENCE FACIAL IMAGES FOR MRTD<br>Version: 1.0 Date – 2018-04, International Civil Aviation Organization |
| 11. | [ISO-3D] | ISO/IEC 19794-5:2005/AMD 2:2009 Three-dimensional face image data interchange format |

**(EXHIBIT E)**

# FPOTUS After Action
# Beaver County ESU/SWAT

# Materials Provided by Butler Command

Materials Provided by Butler Command



# Timeline

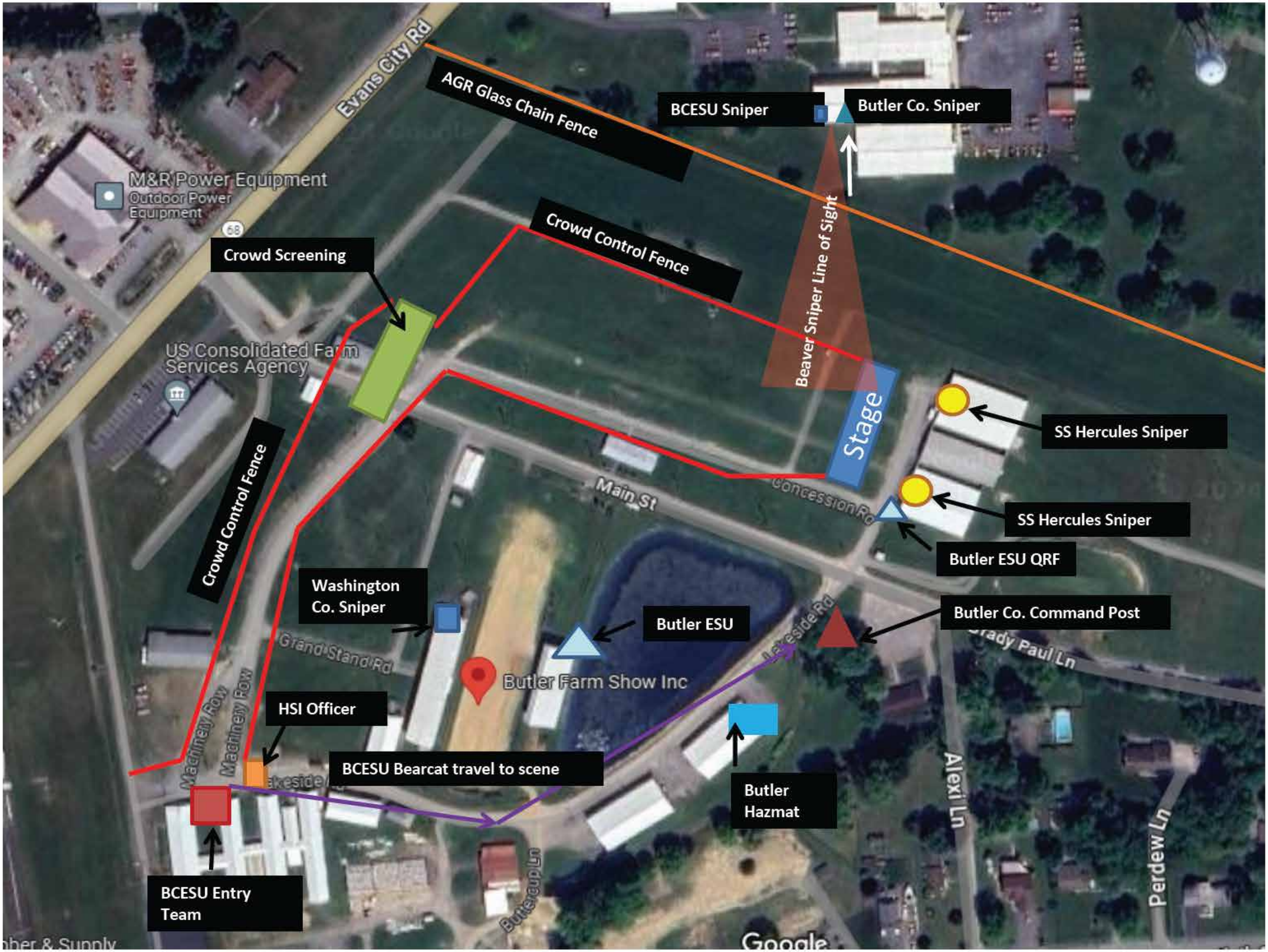
- 0900 – Briefing by Butler Co. ESU
  - Washington Co. ESU
  - Beaver Co. ESU
  - Butler Co. ESU
  - State Police – no input
  - Bravo Team Leader Gives Assignments
- 10:15 – Beaver Co ESU in place
- 10:30 – Vendor dispute at Main Entrance handled by Butler Co Sheriff Slupe
- 10:30 – Snipers in place
- 17:10 – First Observed Suspect by Nicol
  - Walked by window
- 17:14 – Picture of Suspect (time taken)
- 17:28 – Picture of Bike (time taken)
- 17:32 – Suspect spotted looking at phone, news feeds, and range finder confirmed through monoculars

# Timeline

- 17:34 (approx.) – Butler Co. Sniper texts Butler  Team(assumed)
- 17:38 – Nicol sends text to group text to Sniper Group about suspect
- 17:40 – Response text to Nicol “Call into command”
- 17:41 – Called into command by Nicol about suspect (Butler 4 Command Frequency)
  - 4 Sierra 2 to Command – communicated description and range finder lurking around AGR Building
- 17:45 – Text sent to Beaver ESU Group Command about Suspect and to relay to command
- 17:49 – Priolo communication to Denny Crawford regarding suspect and pictures
- 17:55 – Crawford acknowledges receipt to Priolo and passing it on to command
- 17:59 – Crawford to Priolo sent to Command and asking for direction of travel
- 18:00 – Priolo to Nicol asking for direction of travel for suspect
- 18:00 – Nicol to Priolo unsure of direction of travel
- 18:05 – Approx  suspect at picnic tables and moving direction of Sheetz, he has a back pack (communicated by Nicol) via radio
  - Bulter Sniper stayed in place at original position

# Timeline

- 18:06 – 18:12:
  - Nicol goes downstairs of building 1 to meet patrol to let them know suspect is around building on side of fairgrounds
    - 1 Marked vehicle and unmarked vehicle pull in together
- 18:12 – Shots Fired
- Unknown Time: Shooter Down
- 18:23 – (approx.) Vasiladitois-Nicol and Gianvito climb black tactical ladder to L of Building 3 door to access roof
- 18:25 – Pronounced DOA by Vasiladiotis-Nicol
- 18:25 – General clearing by Beaver County ESU with other agencies of surrounding buildings
- 18:32 – DOA Photo sent by Gianvito sent to Shane and Patrick
- 18:35 – Gianvito sends confirmation picture to command to confirm dead
- 18:46 – Schaffer from Washington Co. ESU pats suspect down finds cellphone and device
- 18:48 – Cellphone and remote found in deceased's right pocket sent to Shane
- 19:45 – Device and Face sent by Gianvito. Number provided by EOD.
  - [redacted] sent phone number
- 19:46 – Facial recognition photo sent by Gianvito to [redacted]



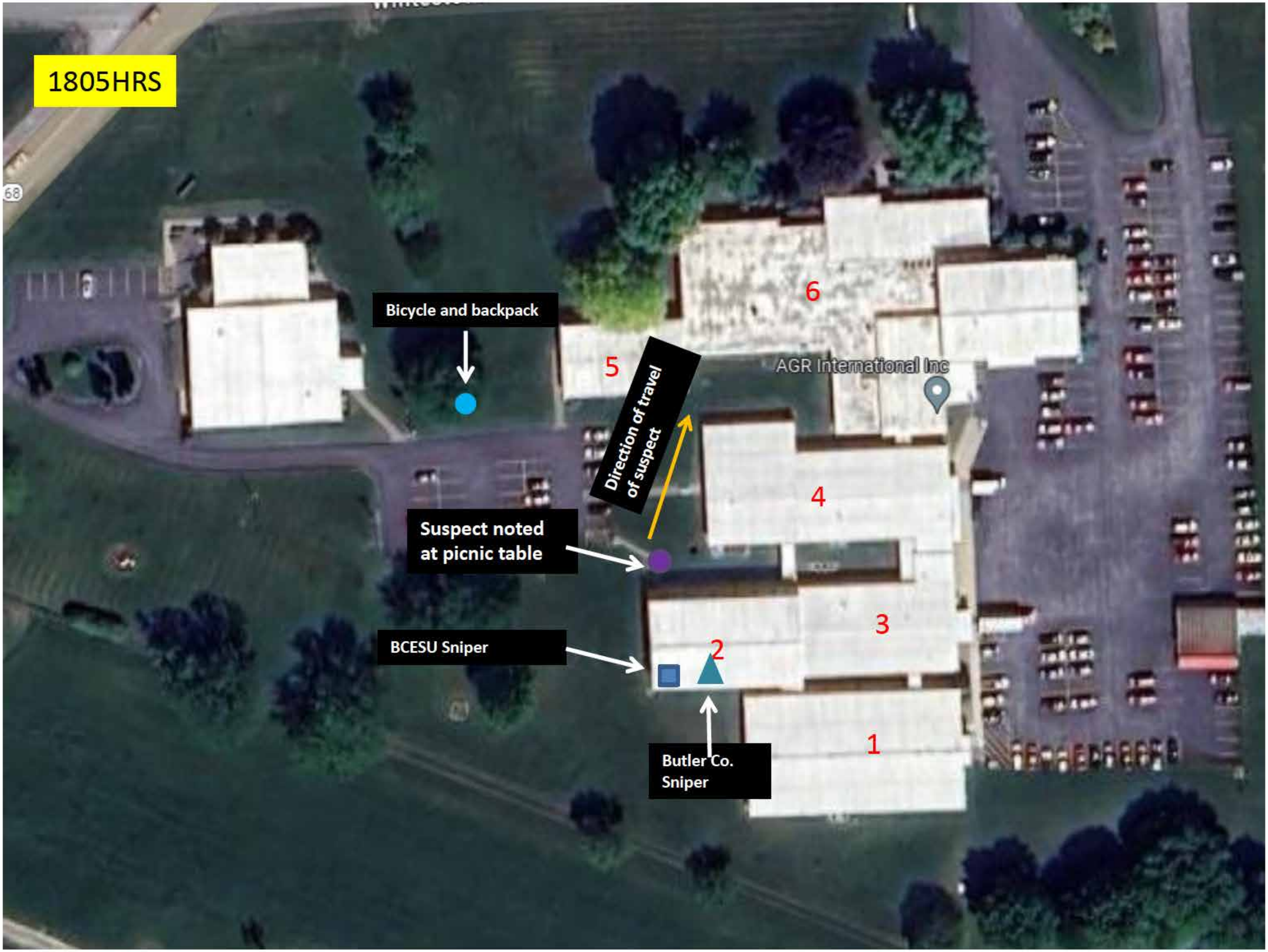
Evans City Rd
AGR Glass Chain Fence
BCESU Sniper
Butler Co. Sniper
M&R Power Equipment
Outdoor Power Equipment
68
Crowd Screening
Crowd Control Fence
Beaver Sniper Line of Sight
US Consolidated Farm Services Agency
Stage
SS Hercules Sniper
Crowd Control Fence
Main St
Concession Rd
SS Hercules Sniper
Butler ESU QRF
Washington Co. Sniper
Butler ESU
Butler Co. Command Post
Lakeside Rd
Grady Paul Ln
Grand Stand Rd
Butler Farm Show Inc
Machinery Row
Machinery Row
HSI Officer
BCESU Bearcat travel to scene
Butler Hazmat
Alexi Ln
Perdew Ln
Buttercup Ln
BCESU Entry Team
Google


1710HRS
68
AGR International Inc
1
2
3
4
5
6
BCESU Sniper
Suspect first spotted
Butler Co.
Sniper

Suspect Photo
Taken by: G. Nicol
Captured: 07/13/2024 17:14
Sent to: Sniper Group and BCESU
Commander Group

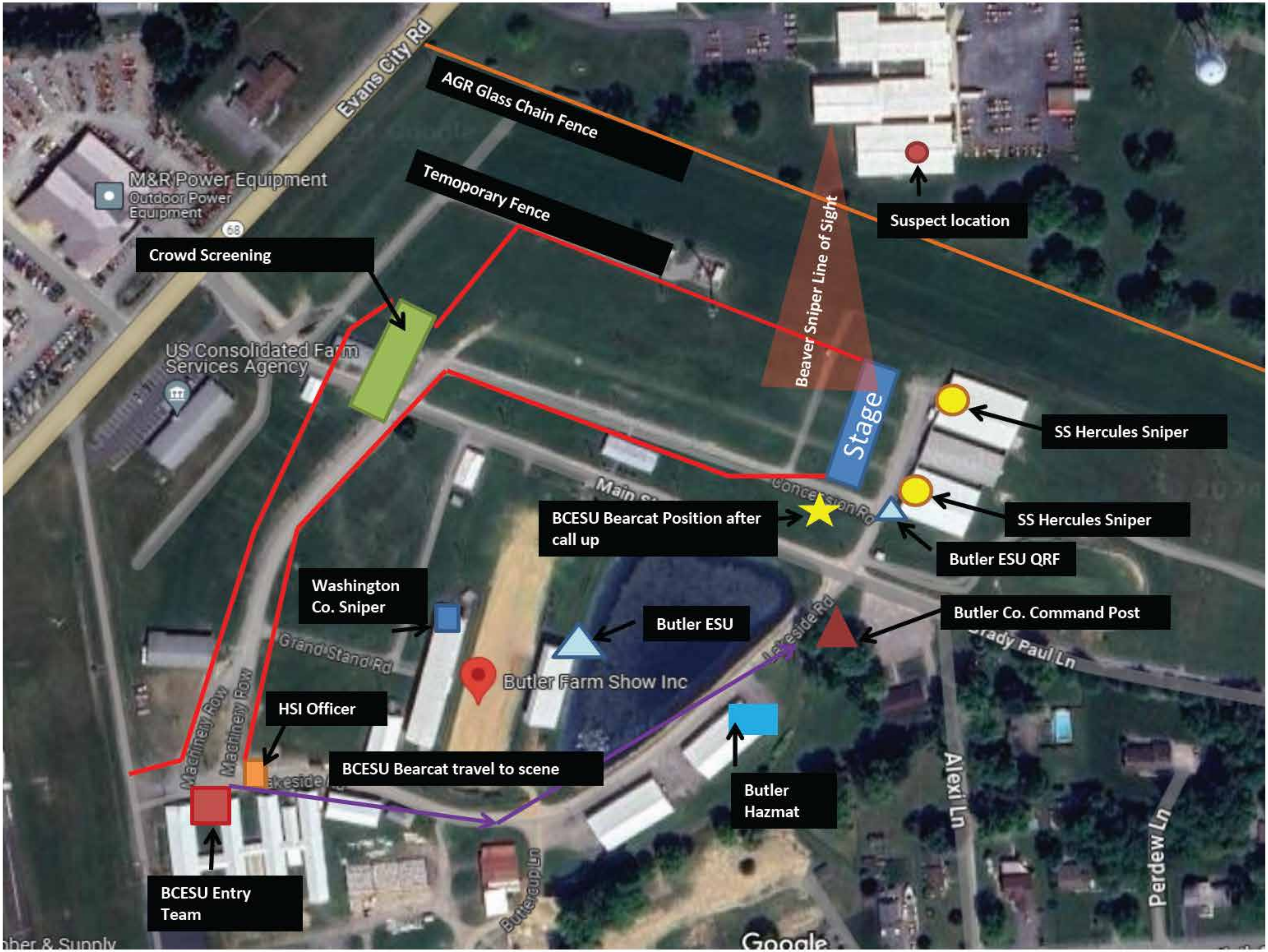
Photo of Bicycle and Backpack
Taken by: G. Nicol
Captured: 07/13/2024  17:28
Sent to: BCESU Commander Group


1732HRS
Bicycle and backpack
6
5
AGR International Inc
4
3
2
1
BCESU Sniper
Suspect first spotted
Butler Co.
Sniper
68

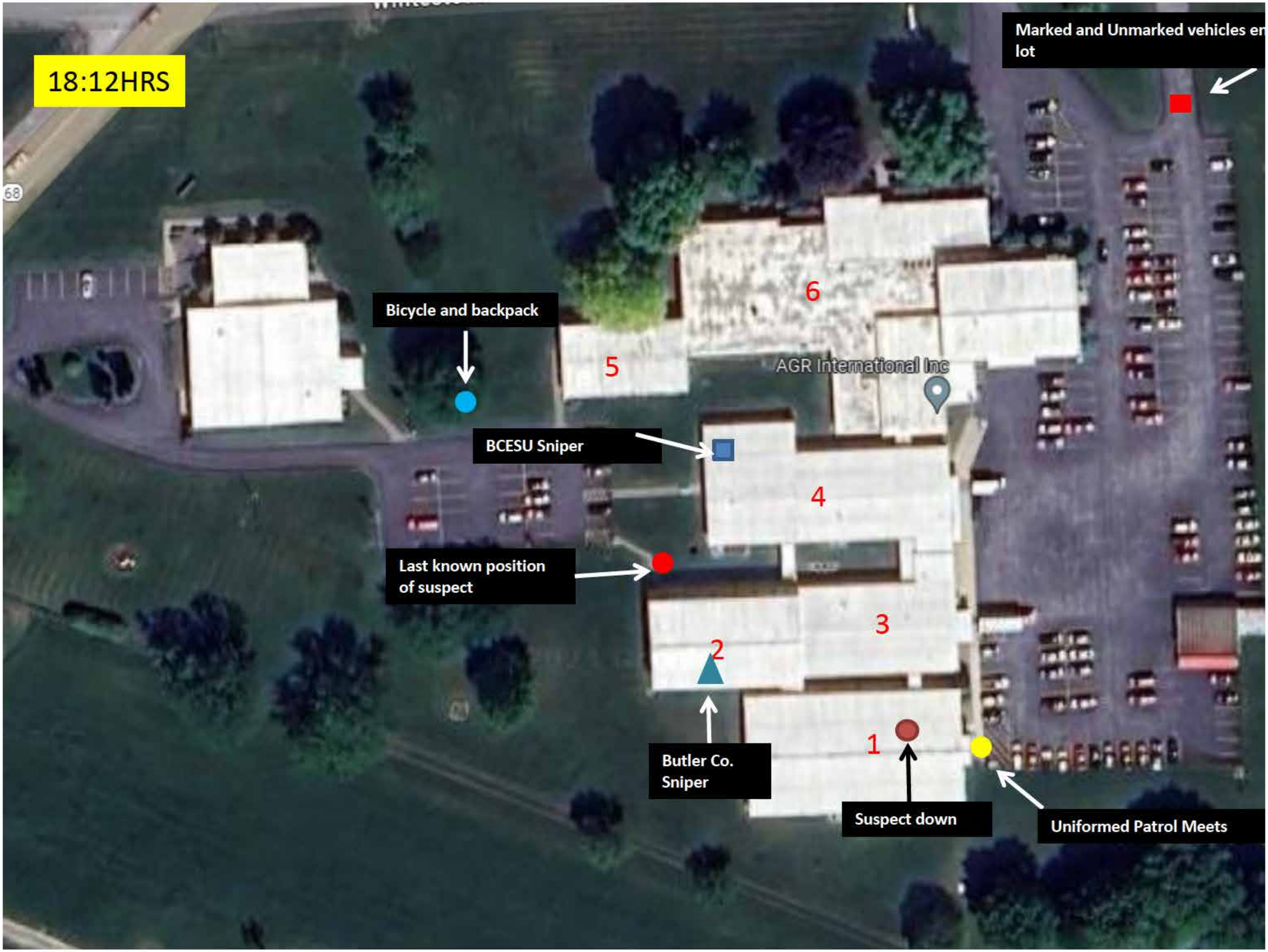

1805HRS
Bicycle and backpack
AGR International Inc
6
5
Direction of travel of suspect
4
Suspect noted at picnic table
3
BCESU Sniper
2
1
Butler Co. Sniper


1806-18:11HRS
Marked and Unmarked vehicles en
lot
Bicycle and backpack
6
5
AGR International Inc
4
3
2
1
BCESU Sniper
Butler Co.
Sniper
Uniformed Patrol Meets

SHOTS FIRED
18:12HRS

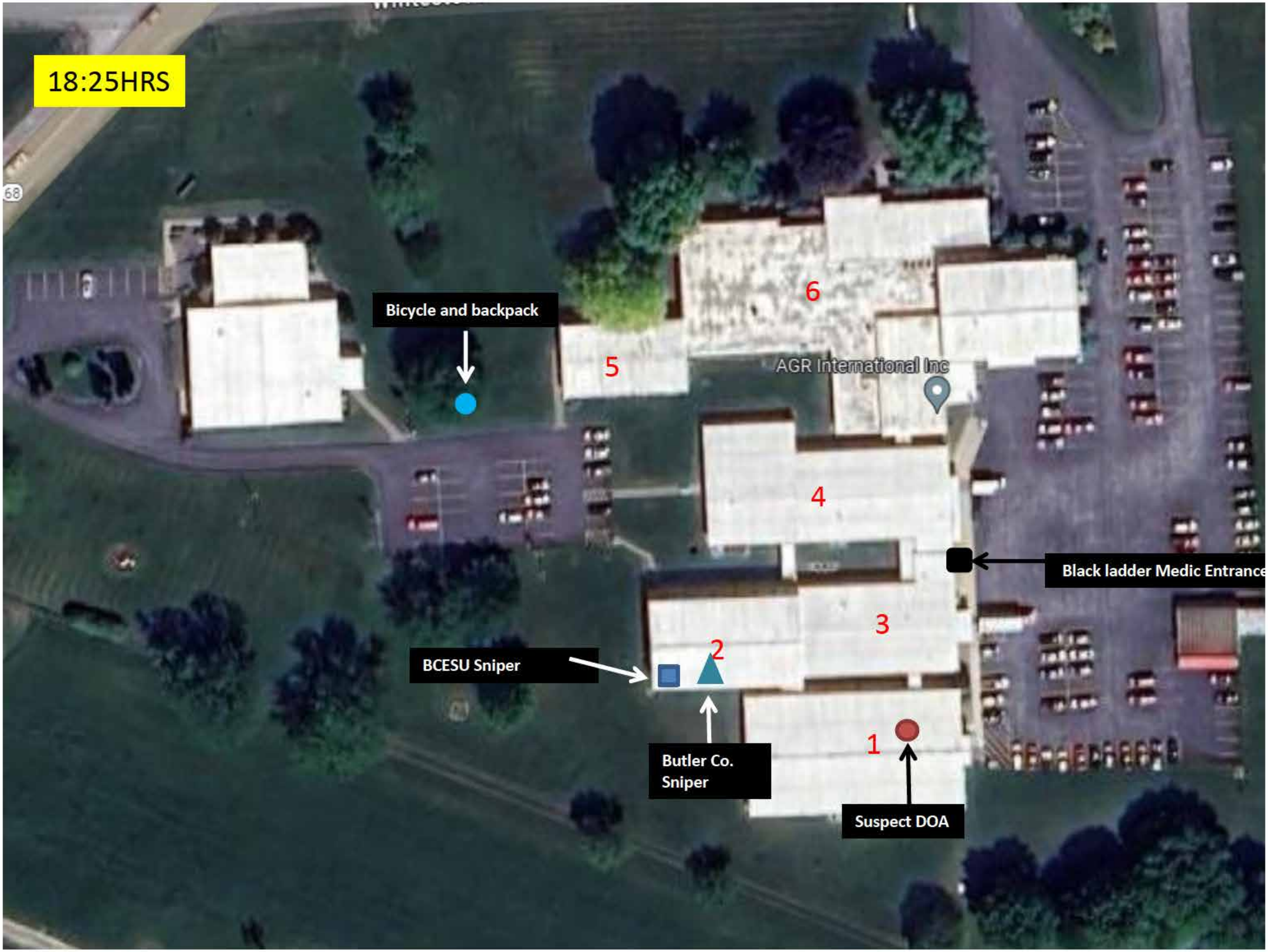


AGR Glass Chain Fence
Temoporary Fence
Evans City Rd
M&R Power Equipment
Outdoor Power Equipment
Crowd Screening
US Consolidated Farm Services Agency
Beaver Sniper Line of Sight
Suspect location
Stage
SS Hercules Sniper
SS Hercules Sniper
BCESU Bearcat Position after call up
Butler ESU QRF
Washington Co. Sniper
Butler ESU
Butler Co. Command Post
Grand Stand Rd
Butler Farm Show Inc
Lakeside Rd
Brady Paul Ln
HSI Officer
BCESU Bearcat travel to scene
Butler Hazmat
Machinery Row
Alexi Ln
Perdew Ln
Buttercup Ln
BCESU Entry Team
Google



18:12HRS
Marked and Unmarked vehicles en
lot
6
5
AGR International Inc
Bicycle and backpack
BCESU Sniper
4
Last known position
of suspect
3
2
Butler Co.
Sniper
1
Suspect down
Uniformed Patrol Meets
68

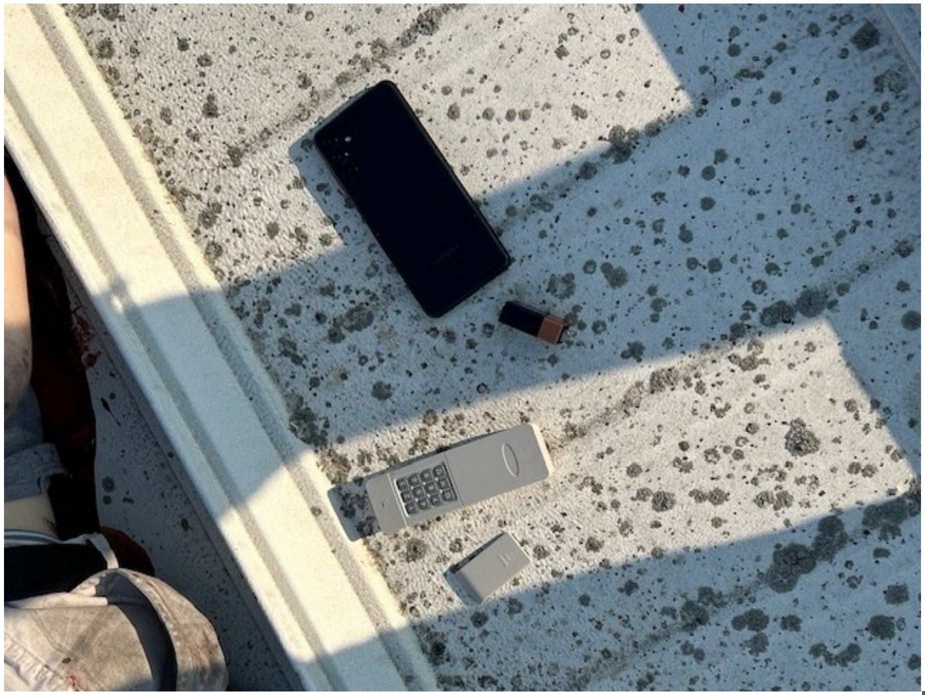
Vasiladiotis-Nicol and Gianvito make access to Roof
Time: 18:23 approx.



18:25HRS
Bicycle and backpack
5
6
AGR International Inc
4
Black ladder Medic Entrance
3
2
BCESU Sniper
Butler Co.
Sniper
1
Suspect DOA

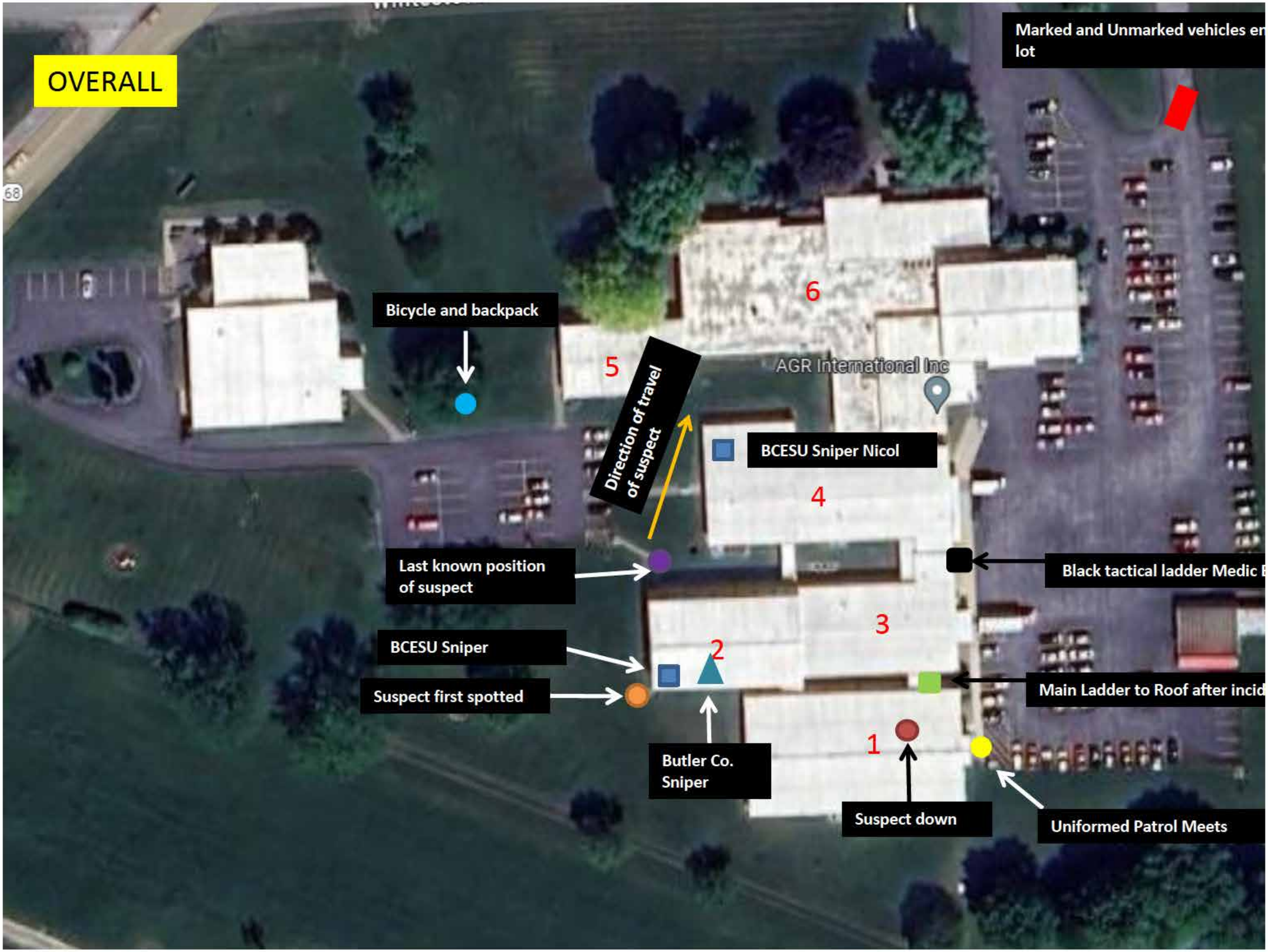
DOA Confirmation Photos
Taken by: Gianvito

Captured: 07/13/2024  18:32
Sent to: R.P. Young and Shane



Device and Phone Photos
Taken by: Gianvito
Captured: 07/13/2024  19:45
Sent to: [redacted]
Requested By: EOD

Facial Recognition Photo
Taken by: Gianvito
Captured: 07/13/2024 19:46
Sent to: [redacted]
Requested By: EOD



OVERALL
Marked and Unmarked vehicles en
lot
68
Bicycle and backpack
6
5
AGR International Inc
Direction of travel of suspect
BCESU Sniper Nicol
4
Last known position of suspect
Black tactical ladder Medic E
3
BCESU Sniper
2
Suspect first spotted
Main Ladder to Roof after incid
Butler Co. Sniper
1
Suspect down
Uniformed Patrol Meets

# Duties

- Shane Monitor Channel 4 – Butler Police ESU Command
- Priolo Monitor Channel 3 – Butler Police Patrol
- Sniper:
  - G. Nicol
- Operators
  - J. Oshe
  - T. Shane
  - M. Priolo
  - A. Bitts
  - R. Gianvito
  - R. Costanza
  - R.P. Young
- Medic
  - Vasiladiotis-Nicol