Scientific Working Group on Digital Evidence

Best Practices for Data Acquisition from Digital Video Recorders

17-V-002-1.3

The version of this document is in draft form and is being provided for comment by all interested parties for a minimum period of 60 days.

Disclaimer Regarding Use of SWGDE Documents

SWGDE documents are developed by a consensus process that involves the best efforts of relevant subject matter experts, organizations, and input from other stakeholders to publish standards, requirements, best practices, guidelines, technical notes, positions, and considerations in the discipline of digital and multimedia forensics and related fields. No warranty or other representation as to SWGDE work product is made or intended.

SWGDE requests notification by email before or contemporaneous to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in such proceeding. The notification should include: 1) The formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; and 3) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Subsequent to the use of this document in the proceeding please notify SWGDE as to the outcome of the matter. Notifications should be submitted via the SWGDE Notice of Use/Redistribution Form or sent to secretary@swgde.org.

From time to time, SWGDE documents may be revised, updated, deprecated, or sunsetted. Readers are advised to verify on the SWGDE website (https://www.swgde.org) they are utilizing the current version of this document. Prior versions of SWGDE documents are archived and available on the SWGDE website.

Redistribution Policy

SWGDE grants permission for redistribution and use of all publicly posted documents created by SWGDE, provided that the following conditions are met:

1. Redistribution of documents or parts of documents must retain this SWGDE cover page containing the Disclaimer Regarding Use.
2. Neither the name of SWGDE nor the names of contributors may be used to endorse or promote products derived from its documents.
3. Any reference or quote from a SWGDE document must include the version number (or creation date) of the document and also indicate if the document is in a draft status.

Requests for Modification

SWGDE encourages stakeholder participation in the preparation of documents. Suggestions for modifications are welcome and must be submitted via the SWGDE Request for Modification Form or forwarded to the Secretary in writing at secretary@swgde.org. The following information is required as a part of any suggested modification:

DRAFT

a) Submitter's name
b) Affiliation (agency/organization)
c) Address
d) Telephone number and email address
e) SWGDE Document title and version number
f) Change from (note document section number)
g) Change to (provide suggested text where appropriate; comments not including suggested text will not be considered)
h) Basis for suggested modification

Intellectual Property

All images, tables, and figures in SWGDE documents are developed and owned by SWGDE, unless otherwise credited.

Unauthorized use of the SWGDE logo or document content, including images, tables, and figures, without written permission from SWGDE is a violation of our intellectual property rights.

Individuals may not misstate and/or over represent duties and responsibilities of SWGDE work. This includes claiming oneself as a contributing member without actively participating in SWGDE meetings; claiming oneself as an officer of SWGDE without serving as such; claiming sole authorship of a document; use the SWGDE logo on any material and/or curriculum vitae.

Any mention of specific products within SWGDE documents is for informational purposes only; it does not imply a recommendation or endorsement by SWGDE.

DRAFT

Scientific Working Group on Digital Evidence

Best Practices for Data Acquisition from Digital Video Recorders

Table of Contents

1. Purpose 3
2. Scope 3
3. Limitations 3
4. Types of Digital Video Recorders (DVR), Cameras, and Management Systems 4
   - 4.1 Stand-Alone Embedded Digital Video Recorder 4
   - 4.2 Network Video Recorder (NVR) 4
   - 4.3 Hybrid Digital Recorder 4
   - 4.4 Dedicated Computer 4
   - 4.5 Personal Computer 4
   - 4.6 Server Based 4
   - 4.7 Internet Protocol (IP) Camera 4
   - 4.8 Video Management System (VMS) 4
5. DVR Recordings 5
6. Compression 5
7. Legal Considerations 5
8. Recommended Equipment 5
9. Steps to Take Prior to Acquisition 7
10. Steps to Take During Acquisition 7
    - 10.1 Items that should be documented 8
    - 10.2 Documentation 8
11. DVR Outputs 9
    - 11.1 USB Devices 9
    - 11.2 Optical Media Writer 10
    - 11.3 Network Connection 10
    - 11.4 Video Capture Device 11
    - 11.5 Direct Drive Access 11
12. Removal of DVR Unit 12
13. Steps to Take After Acquisition and Prior to Leaving Scene 12

DRAFT

14. References 13
15. Additional Resources 13
16. Appendix A – Sample Audio/Video Field Retrieval Worksheet 14
17. History 15

DRAFT

1. Purpose

The purpose of this document is to provide guidance for acquiring video, audio, and associated data evidence from digital video recorders (DVRs).

These guidelines may also be used to assist organizations when developing standard operating procedures (SOPs) for the acquisition of video and audio evidence from digital video recorders.

2. Scope

This document provides guidance for the acquisition of evidence utilizing a DVR's operating system to export the native or proprietary data for use in a criminal investigation and/or prosecution. Information can be obtained from consumer-grade DVRs without specialized technical knowledge but may cause information to be lost (e.g., metadata, multiple cameras) or degraded (e.g., raster size, frame rate) without specialized technical knowledge. This document identifies a forensic workflow for the acquisition of data from such devices. The purpose of this workflow is to extract the best evidence and ensure data integrity. For the purposes of this document the term DVR encompasses all types of digital video recorders (e.g., NVR, hybrid)

3. Limitations

The responding individual should have some knowledge of DVRs and a basic understanding of video evidence. This document is not intended to be an exhaustive guide for field personnel who do not have experience acquiring video evidence nor to replace organizational policy or standard operating procedures, nor should it be construed as legal advice. Legacy digital outputs are not described in this document; for more information on these options, see *SWGIT Section 24 Best Practices for the Retrieval of Digital Video*.

This document describes procedures for acquiring data of evidentiary value from consumer-grade DVRs. Methods of retrieval from IoT devices are addressed in *SWGDE 23-F-004-1.0 Best Practices for Digital Evidence Acquisition from Cloud Service Providers* [1].

In cases where exporting the data from the device in the field is not practical or feasible, data recovery may require removal of the recording device and the inclusion of a computer forensic examination workflow.

This document may not be applicable in all circumstances. When warranted, a collector may deviate from these best practices and still obtain reliable, defensible results. If collectors encounter situations warranting deviation from best practices, they should document the specifics of the situation and actions taken.

This document does not address all safety-related concerns for the collection of electronic devices. Safety measures should be in place, and compliance with departmental standards and SOPs for potential hazards. This includes power-related peripheral devices that malfunction or could cause harm to the responding individual. This includes grounding devices and an awareness of conditions in which the DVR was seized (e.g., transformers, environmental factors, physical damage).

4. Types of Digital Video Recorders (DVR), Cameras, and Management Systems

Digital video recorders are primarily found in residential, commercial, or governmental institutions and include these major types:

4.1 Stand-Alone Embedded Digital Video Recorder

Menu-driven device containing a recording system that typically uses a proprietary operating system to convert an analog video signal to digital data and store it.

4.2 Network Video Recorder (NVR)

Menu-driven device containing a recording system connected to IP cameras that typically uses a proprietary operating system to accept a digital stream and store it (the conversion from an analog source to a digital stream at the camera or an encoder prior to reaching the NVR).

4.3 Hybrid Digital Recorder

Menu-driven device capable of recording both a network (digital) video stream and/or an analog signal.

4.4 Dedicated Computer

PC-based proprietary system dedicated to recording video.

4.5 Personal Computer

Standard personal computer running video recording software and likely other software.

4.6 Server Based

Network attached storage (NAS) that may be storing video either locally or remotely.

4.7 Internet Protocol (IP) Camera

IP cameras utilize an internet connection that allows for remote access through a web client or mobile application. They may not store video, and the user may only access/view a live video and/or audio stream, they may have the capability of recording multimedia to the cloud, or a SD card on the camera as the primary recording or as a backup recording.

4.8 Video Management System (VMS)

Software used to monitor, control, and record various entities connected to the system. Entities include but are not limited to the following: cameras, access controls, license plate inputs. These entities are typically connected to physical servers located on the premises or cloud-based servers off premises.

DRAFT

5. DVR Recordings

When acquiring video evidence, the goal is to obtain the most accurate data and image quality from the DVR. Most DVRs allow for the export of data. Consideration should be given to the following:

- The evidence from DVRs is perishable and should be acquired as soon as possible.
- In some cases, an open file format and a native file format will both be available for export. A native file format or proprietary file format is likely to provide best evidence for legal authenticity purposes as it is closest to the original manner of recording.
    - Additionally, the proprietary player and/or codec should be acquired directly from the device or through the manufacturer.
    - A secondary export of the open file format should also be acquired if time is available.
- A review of the retrieved video from all relevant cameras and time periods should be performed to confirm proper playback and to ensure the incident(s) are properly captured.[1]

6. Compression

Compression encodes data to reduce the amount of storage used within the DVR. DVRs vary in the amount and type of compression applied to the recordings. Compression settings are usually chosen when the DVR is initially configured. The compression settings should be documented before acquisition. Adjusting the settings during acquisition is not recommended as it will not improve the quality of the video that has already been recorded.

- A review of the live monitor may appear to be of better quality than the actual recorded video because compression has not yet occurred.
- For more information, an explanation of compression and issues pertaining to it can be found within *SWGDE 17-V-001-1.3 Technical Overview of Digital Video Files*.

7. Legal Considerations

Proper legal authority shall be obtained before acquiring video evidence from a DVR.

8. Recommended Equipment

The following is a list of equipment that may assist with the acquisition of multimedia evidence from DVRs (**bold** text indicates priority equipment):

Devices:

- **Portable computer** with:

[1] Note: When possible, the review should be completed on scene.

DRAFT

    - **Administrator rights**
    - **Capability to install proprietary viewers**
    - **No restrictions that would impede the download** (e.g., firewalls, organization software, group policies)
    - **USB ports**
    - **Optical media drive** (may be peripheral or built-in)
    - **Network port (RJ45)**
- Analog and/or HDMI to USB capture device
- Write blocker
- Wired and wireless USB mouse
    - Some DVRs require a wired mouse, whereas a wireless mouse is more convenient for out-of-reach storage locations.
- Monitor
- USB keyboard

Media:

- Optical disc media
- USB flash drives[2]
- External hard drives (HDD)

Cables:

- Composite cables
- USB extension cable
- Network cable
- BNC to RCA adapters
- VGA to DVI adapter
- HDMI Cable

Other items:

- **Digital camera**
- Flashlight
- Mirror

[2] Note: See section 11.1 for additional information on the preparation of various storage sizes when using USB devices for connectivity to specific devices.

- Archival media markers[3]
- Batteries: variety of sizes
- Power strip and extension cord
- Gloves
- Documentation (e.g., chain of custody forms, consent forms, search warrant)
- USB splitter
- Ladder
- Phillips, flathead screwdrivers, pair of pliers
- Evidence packaging

9. Steps to Take Prior to Acquisition

- Determine the physical location of the recording device. The recorded video may be stored at a remote location rather than the scene of the incident. It is preferable to acquire video data directly from the primary recording device rather than through a remote connection or viewing app.
- Obtain legal authority, if necessary.
- A review of an owner's manual may assist with acquisition (e.g., passwords, output options)
- Determine whether the relevant video is still on the DVR.
- Locate and view the relevant video.
- Determine how much data needs to be acquired (this can sometimes be limited by the search warrant).
- Determine the best method for acquisition.
- To prevent tampering, consider isolating the device from any outside network connection; however, do not disconnect active IP cameras.
- Consider disabling any additional monitors, as they may also display the events and allow others to view sensitive video.

10. Steps to Take During Acquisition

Notes should be kept during the acquisition process (see Appendix A: Sample Audio/Video Field Retrieval Worksheet at the end of this document for an example). Photographs or a recording of the system and settings may also be used in lieu of, or in addition to, written notes.

[3] To prevent physical damage, fine point, roller ball, and solvent-based permanent ink markers should not be used for labeling optical media discs; use water- or alcohol-based ink markers that are designed specifically for this purpose [3].

10.1 Items that should be documented

- Scene contact information:
  - Scene address
  - Scene point of contact and telephone number
- Type of DVR
  - Make, model, and serial number of DVR
  - DVR password(s) and username(s)[4]
- Number of cameras capable of recording and number of cameras connected
- System time/date vs Government-standardized atomic-clock time/date (document device used for actual time and date)[5]
  - Calculate if there is a time offset between real time and the DVR system clock.
    - Applications are available for smart devices that will assist with the offset calculations.

10.2 Documentation

Consider documenting the following items, if applicable.

- Number of microphones capable of recording and number of microphones connected
- Earliest recorded date/time
- Storage capacity/storage used
- Whether overwrite is enabled or set to stop if HDD is full
- If the device is set to delete and reset on a schedule
- System settings:
  - Image quality (e.g., high, medium, low)
  - Frames per second
  - Recorded image/frame size (e.g., 320 x 240)
  - Alarm or motion trigger settings for cameras
- System firmware version
- System logs include any log information offered within the DVR system
- Logs may be exported directly or documented through photographs of the system display, depending on the system[6]

[4] Note: Some user accounts may have elevated or restricted rights. Access to a user account with no restrictions, oftentimes an administrative user, will provide unrestricted access to the DVR data.

[5] Note: Do not change the time and date on the DVR system.

[6] Note: Log *information* may provide useful information about the activities within the system if the video(s) are not available at the time of acquisition.

DRAFT

- Photograph the DVR system, cameras, and connections or sketching camera placement (if necessary)

11. DVR Outputs

- Each acquisition method may offer advantages or disadvantages. Factors that contribute to which output option that is optimal for extraction of the best evidence for legal authenticity purposes. Some available factors that should be considered include:
  - The amount of evidence to be collected
  - Cropping
  - Chroma Subsampling
  - Frame rate
  - Field order
  - Audio and Video Synchronization
- DVRs that record in a proprietary file format may use an associated viewer application for playback of output files. The examiner may have to manually select this option to copy the viewer along with video files.
- Some DVR systems limit the amount of data that can be retrieved (e.g., downloaded, exported) at a time. This limit may not be specified in the system manual or known to the manufacturer.

11.1 USB Devices

Generally, the DVR's software will have an archive, backup, copy, or export function with which you can export/download the data directly to the device attached. If the DVR does not recognize the USB device:

- Formatting the attached USB device using the DVR's operating system may be necessary. Formatting attached devices may be a DVR menu option. Furthermore, older DVR systems must format the removable storage media in order to write data to it.[7]
- The USB device's capacity may be too large for the DVR to recognize. Older DVRs may not recognize devices larger than 2 GB, consider trying another USB device of a smaller capacity.
- A broken USB port may also prevent USB devices from being read or recognized by the DVR. An indicator light on the USB drive, if present, may help to determine if the port is functional.

[7] Note: Formatting a device removes all the current data stored on the device and prepares the device for media storage.

- Some USB ports are specifically designated for a mouse. If the examiner plugs a flash drive into a port and it is not recognized by the DVR, attempt moving the device to another USB port.

11.2 Optical Media Writer

Older DVRs may have an optical writer to output recorded data. Generally, the DVR's software will have an archive, backup, copy, or export function with which one can output data directly to the optical writer. Write-once optical media should be used in preference to rewritable optical media.[8]

If the data is written to rewritable media, transfer the data to non-rewritable media or secure electronic storage as soon as possible. The transfer should be verified according to the methods outlined in *SWGDE 17-I-001-1.0 Best Practices for Maintaining the Integrity of Imagery* [2].

11.3 Network Connection

Many DVRs have network ports and are running a web server application. Furthermore, many DVRs have their own proprietary network viewer software that allows for playback and exporting of the recorded data.

A computer can be connected to the DVR with an ethernet cable to export the recorded video or export logs. Prior to transfer, the network viewer software may need to be installed on the connected computer, although some DVRs will have the viewer available through a web browser. Any setting(s) changed to facilitate connectivity should be made on the destination computer, if possible, rather than on the DVR.

- Network viewers may only allow for viewing the video or the download of an open file format.
- The IP address can usually be obtained from the DVR menu. Some network viewers are installed on the DVR system for easy access. Otherwise, searching the vendor's website or contacting the vendor directly may be necessary.
- If a network viewer for the system does not exist, a connection may be possible utilizing Windows Explorer, or other web browser, and typing in an appropriate IP address.
- One may need to change security settings on the browser to transfer the data.
- Document the original IP address of the DVR as well as any changes made. Some DVR systems have a limitation on the amount of data that can be transferred.
- Some network connected appliances use default streaming protocols to view and encode multimedia streams. This stream may be downgraded due to bandwidth limitations (e.g., higher compression, lower resolution, lower frame rate). The examiner should evaluate

[8] Note: Some older DVRs may only accept a rewritable disc.

the physical recording and storage equipment on the scene for the availability of highest quality recording.

11.4 Video Capture Device

If the video is viewable from the DVR but cannot be exported before leaving the scene the video should be captured or recorded using one of the methods below (listed in order of preference):

- Video Grabber (Hardware) captures and converts the video signal from the DVR. This method does not capture the metadata from the DVR.
- Digital video camera on a tripod (to stabilize the video and reduce shake from users' movement). If possible, one should disable the audio in digital video recordings or inform persons at a scene that an audio recording is being captured. This method does not capture any metadata from the DVR.

11.5 Direct Drive Access

In circumstances where the DVR is damaged, a large amount of video is to be exported, the admin username and password are not known, or a unique investigative circumstance arises, it may become necessary to access the hard drive directly to obtain the video recordings. The best practices for preservation and collection of digital evidence advise that a disk image should be created of the storage drive. The following considerations should be evaluated prior to creating a disk image:

- Investigative time constraints
- Size of the data to be collected
- Size of the storage drive(s)
- Safety of the personnel
- Your organization storage SOPs advise otherwise[9]

The following should be performed:

- Prior to shutting the device off, the examiner should consider obtaining a video capture of times of interest, using a static camera that includes the entire video framing or screen. This recording will serve as a backup in the event that the DVR fails to operate properly when repowered.
- Prior to shutting the device off, the examiner should calculate and document the date and time offset.
- Deactivate the device's power prior to connecting peripheral devices to the hard drive.
- Record the details of the connected hard drive.
- Record the details of the write blocker you are using to connect to the hard drive.

[9] Note: This should only be done with the use of a write blocker to prevent writing to the DVR's storage drive.

- The settings of the DVR are retained on the device, not the hard drive, as such they should be documented.

23.5.1 Removal of Hard Drive

In certain scenarios, extracting the hard drive(s) from the DVR and utilizing reverse engineering software can be an efficient approach to retrieve the desired video footage. However, it is important to be aware of the potential risks associated with this method, which may include:

- DVR Repairs: Removing the hard drive(s) from the DVR for extraction purposes could require subsequent repairs to ensure the DVR continues to function properly. This is necessary to maintain its operational integrity after the extraction process.
- Unrecognized Video Format: There is a possibility that the video format stored on the extracted hard drive(s) may not be readily recognized by the software or devices used for retrieval. In such cases, the traditional method of retrieval through the DVR GUI would have to be used.
- DVR Hard Drive Reformatting: When the extracted hard drive(s) are returned to the DVR after the video retrieval process, there is a risk that the DVR might initiate a reformatting procedure. This could potentially erase the retrieved video footage, resulting in the loss of the desired content.

It is crucial to consider these potential risks and plan accordingly when opting for this method of video retrieval. Adequate measures should be taken to address any repairs required, ensure compatibility with the video format, and prevent unintended reformatting of the hard drive(s) by the DVR upon reinstallation.

For more information related to computer forensic examinations of the storage device, see *SWGDE 18-F-001-1.0 Best Practices for Computer Forensic Examinations*.

12. Removal of DVR Unit

In certain circumstances, it may be necessary to seize the DVR. Examples include:

- The amount of video evidence is too large to be downloaded on scene
- The output ports on the DVR are not functional
- The examiner is not able to gain full logical access to the device
- Personnel safety is at risk
- The DVR may need to be seized to protect the evidence, or if continued access could impact an ongoing investigation
- Acquisition of data directly from the hard drive is the most appropriate way to obtain relevant data and metadata
- All other attempts to export data have failed

13. Steps to Take After Acquisition and Prior to Leaving Scene

Complete all the necessary documentation.

- Initiate a chain of custody for the evidence, per organizational policies
- Collect all required video data and proprietary playback software/codec(s)
- Verify the acquired video evidence plays back correctly on the portable computer and that the correct dates and times were retrieved
- The recording system has been returned to its original state (i.e., any changes to the system settings have been restored)
- Any evidence stored on a temporary storage device (e.g., USB drive, rewritable media) should be transferred to a permanent storage device

Refer to *SWGDE 17-I-001-1.0Best Practices for Maintaining the Integrity of Imagery* [2] and organizational SOPs for guidance on securing and authenticating acquired data.

14. References

[1] Scientific Working Group on Digital Evidence. *Best Practices for Digital Evidence Acquisition from Cloud Service Providers*. SWGDE 23-F-004-1.0. *SWGDE*, 2023, https://www.swgde.org/23-f-004/.

[2] Scientific Working Group on Digital Evidence. *Best Practices for Maintaining the Integrity of Imagery.* SWGDE 17-I-001-1.0. *SWGDE*, 2017, https://www.swgde.org/17-i-001/.

[3] Council on Library & Information Resources. "Conditions That Affect CDs and DVDs." *CLIR*, 2003, https://www.clir.org/pubs/reports/pub121/. Accessed 26 Jan. 2017.

15. Additional Resources

- Scientific Working Group on Digital Evidence. *Best Practices for Computer Forensic Examinations*. SWGDE 18-F-001-1.0. *SWGDE*. 2018, https://www.swgde.org/18-f-001/.
- Scientific Working Group on Digital Evidence. *Technical Overview of Digital Video Files*. SWGDE 17-V-001-1.3. *SWGDE*, 2017, https://www.swgde.org/17-v-001/.
- Scientific Working Group on Imaging Technology. *Section 24: Best Practices for the Retrieval of Digital Video*. Version 1.0, *SWGDE*, 2013, https://www.swgde.org/swgit_24/.

DRAFT

16. Appendix A – Sample Audio/Video Field Retrieval Worksheet

AUDIO/VIDEO FIELD RETRIEVAL FORM

Incident #: _____ **Offense Type:** _____

Location (Address): _____

Scene Point of Contact: _____

Scene Point of Contact Telephone Number: _____

Date & Time of Offense: _____

Date & Time of Acquisition: _____

Date & Time– Actual: _____ **Date & Time– DVR:** _____

DVR Recording Date & Time Difference to Actual (Time Offset): _____

DVR Type & Manufacturer: _____

DVR Model #: _____ **DVR Serial #:** _____

DVR Username: _____ **DVR Password:** _____

ADDITIONAL INFORMATION (IF AVAILABLE):

Earliest Recorded Date/Time: ___ **Manual for DVR available?** ☐ Y ☐ N
Storage Capacity: _____ **Overwrite Enabled:** ☐ Y ☐ N **Firmware Version:** _____
# of Cameras Possible: _____ **# of Cameras Attached to the DVR:** _____
# of Cameras Exported: _____ **Camera Resolution:** ____ **Camera Frame Rate:** ___
Logs Present: ☐ Y ☐ N **Logs Exported:** ☐ Y ☐ N
Image Quality: ☐ High ☐ Medium ☐ Low ☐ Other ___
Camera Settings (e.g. alarm or motion triggered): _____
Starting Date & Time of Selection: _____ **Ending Date & Time of Selection:** _____
Media Backup Format: ___ **Media Copied to: DVD** ___ **CD** ____ **Flash Drive** ____
Other___
Notes:

• Native/proprietary video files should be the highest priority. • Verify video exported on a separate PC prior to leaving the scene, if possible. • Create a hash value for any video retrieved. • Begin Chain of Custody immediately. • Properly label and protect all electronic evidence. • DO NOT USE BALL POINT PENS or stickers on optical media. • Fill out as much information as you have available on this form. • Retain this form as part of the case file.

DRAFT

17. History

Revision	Issue Date	History
1.0 DRAFT	8/24/2017	Initial draft created and SWGDE voted to release as a Draft for Public Comment.
1.0 DRAFT	10/17/2017	Formatted for release as a Draft for Public Comment.
1.0	1/11/2018	Minor grammatical changes and added additional reasons to Section 12. SWGDE voted to release as a Final Approved Document.
1.1 DRAFT	1/10/2023	Updated resources to stay current and clarified definitions as part of the five-year review.
1.2 DRAFT	6/14/2023	Substantive changes made to the direct drive access section with considerations included to obtaining a disk image. Formatting and grammatical changes we also made.
1.2 DRAFT	9/15/2024	Public comments received after final vote, documentation of date/time section required clarification, and the document was released as a draft for public comment.
1.2 DRAFT	1/16/2025	SWGDE voted to release as a Draft for Public Comment.
1.2 DRAFT	2/10/2025	Formatted for release for public comment.

DRAFT