Guidance for the Provision of ESI to Detainees

Joint Electronic Technology Working Group
October 25, 2016

Contents

Guidance 1
I. An Approach to Providing e-Discovery to Federal Pretrial Detainees 1
II. Special Concerns in the Delivery of ESI to Detainees 2
A. Defense Concerns 2
B. CJA and FDO Budgeting Concerns 3
C. Court Concerns 3
D. Facility Concerns 3
E. U.S. Marshals Service Concerns 4
F. Government Concerns 4
III. Practical Steps 4
A. Government, Defense, Facility and Judicial Points of Contact/Working Group 4
B. Identify Facility e-Discovery Capabilities 5
C. Starting Up 6
IV. Special Responsibilities of Participants 6
A. Special Responsibilities of the Government 6
B. Special Responsibilities of the Defense 7
C. Special Responsibilities of the Court 7
D. Special Responsibilities of the Facility 8
E. Special Responsibilities of the U.S. Marshals Service 8
V. Technical Considerations for the Non-Specialist 8
A. Devices and Device Configuration 8
B. Common File Types and Review Possibilities 9
C. Encryption 10
Technical Appendices 11
I. Identification of Installed Software 11
II. E-Discovery Review Laptop Configuration Suggestions 11
A. General Suggestions 11
B. BOP July 2015 Specifications 12
1. Operating System and Software Security Features 12
a. Operating system 12
b. Third-Party Software 12
2. Security Features 13
III. Common File Types and Review Applications 14
A. File Types Listed in the BOP July 2014 Electronic Discovery RFI 14

B. Quick View Plus 13 Professional, Supported File Formats 16
C. Windows Media Player 12 19
D. Litigation Support Database Applications 19

Guidance

I. An Approach to Providing e-Discovery to Federal Pretrial Detainees

After the publication of the 2012 JETWG Recommendations for ESI Discovery in Federal Criminal Cases, the Joint Electronic Technology Working Group turned to specific challenges regarding the delivery of discovery in digital format ("e-discovery" or "ESI"—electronically stored information) to indigent pretrial detainees.[1] Most information is now created, stored, and processed electronically, and most discovery in federal criminal cases is now in digital format. But most facilities that house federal pretrial detainees remain structured to enable detainees to review paper discovery, not digital discovery. With proper safeguards, we believe that the provision of e-discovery to pretrial detainees—inevitable in any event—will also result in greater efficiency, reduced delay, and cost savings for the entire criminal justice system. We believe that facilities must necessarily transition to enabling pretrial detainees to review e-discovery, but we also recognize systemic institutional reasons, often influenced by limited resources, why this evolution from paper-based review to e-discovery review will take time to implement. In the meantime, we have developed some practical guidance for jurisdictions to address the specific challenges in delivering e-discovery in digital format. This Guidance reflects the observations of Government and defense attorneys, litigation support experts, Bureau of Prisons and U.S. Marshal officials, and United States Magistrate Judges, who participated in the project. [2] As with the JETWG Recommendations, this Guidance is intended to be practical, and is not intended to create or define any legal rights. Baseline understandings for the provision of ESI in criminal discovery remain the 2012 JETWG Recommendations. Comments and developments from the field relating to this Guidance may be freely sent to the national points of contact listed later.

---

[1] While this project was initiated with concern for the provision of ESI to indigent detainees, much of what is said here will also be applicable to detainees with retained counsel, because the main limitations on provision of ESI to detainees are not likely to derive from the cost of equipment, but rather from constraints within the facility on the management and use of equipment. At the opposite end of the spectrum, detained defendants who have refused counsel will present additional issues we have not attempted to address in this first edition of this Guidance. That being stated, all stakeholders must recognize their obligations to provide to all pretrial detainees access to their criminal electronic discovery.

[2] Members of the JETWG subcommittee addressing the provision of ESI to detainees include U.S. Magistrate Judges Laurel Beeler (N.D. Cal.) and Jonathan W. Feldman (W.D.N.Y.); Administrative Office of the U.S. Courts, Defender Services Office, National Litigation Support Administrator Sean Broderick; Federal Defender Donna Elm, (M.D.Fla.); Bureau of Prisons Assistant General Counsels Corinne Nastro and Monya Phillip; U.S. Marshals Service Prisoner Operations Division Assistant Chief Heather Lowry; Associate Deputy Attorney General and National Criminal Discovery Coordinator Andrew Goldsmith, Assistant U.S. Attorneys John Haried, Criminal eDiscovery Coordinator at the Executive Office for U.S. Attorneys; John McEnany (S.D.N.Y.); Fred Sheppard (S.D. Cal.); David Joyce (D.Me.); and U.S. Attorney's Office Litigation Support Manager Craig Bowman (W.D.N.Y.).

The U.S. Marshals Service ("USMS") has general responsibility for the custody of federal pretrial detainees. The USMS safeguards approximately 10,000 detainees in Federal Bureau of Prisons ("BOP") facilities; another 10,000 detainees in private facilities under contract to the USMS; and more than 31,000 detainees in approximately 1,800 state and local facilities under USMS contract.[3] Discovery review computers with a standardized configuration are available in most BOP facilities, but there is currently no single standard for ESI review equipment in the state, local and private USMS contract facilities. We do not now foresee development of a single protocol for the provision of ESI to pretrial detainees, given the multitude of facilities; the variety in file format and volume of ESI; the equipment available within, or acceptable to, a given facility; inventory control and technical support staffing within the facility; and other considerations, such as prisoner separations and protective orders. On the other hand, growing experience shows that as long as due regard is given at the local level to the accommodations needed to introduce ESI into a given facility, workable procedures can be developed to handle the common run of e-discovery. This Guidance is intended to aid those necessary accommodations by identifying the specific concerns of each of the various stakeholders, as well as the areas where each stakeholder may need to accept specific responsibilities, to ensure that detained defendants get adequate access to e-discovery in a workable and collaborative manner. This Guidance will also introduce some of the technical aspects of providing ESI to detainees, for example, how, with commonly available software, and some expertise, a PC[4] laptop can be configured to permit review of the most common types of criminal e-discovery.

II. Special Concerns in the Delivery of ESI to Detainees

In preparing this Guidance, we identified the following special concerns in the delivery of ESI to detainees:

A. Defense Concerns

To mount an effective defense, a represented defendant who is detained pending trial must generally have the opportunity to personally review some or all of the discovery and disclosure, which is now commonly in ESI format. The defendant may need to review it in discussion with his counsel or expert as well. But defense counsel may not have the equipment or personnel to do

[3] *See* United States Marshals Service Fact Sheet, Prisoner Operations 2016 and Facts & Figures 2016, available at https://www.usmarshals.gov/duties/factsheets. (Note that the Department of Justice is phasing out the use of private facilities. *See* https://assets.documentcloud.org/documents/3027877/Justice-Department-memo-announcing-announcing.pdf.)

[4] Because the Department of Justice (including the Bureau of Prisons), like most other government agencies, uses PC machines with Windows operating systems, defense teams are encouraged to use PC devices to manage e-discovery. PC devices are typically less expensive than Apple devices; conversion and compatibility issues will be lessened; and problems will be easier to troubleshoot if all parties use PC/Windows devices.

so, and the client who can afford counsel may not be able to additionally pay counsel to bring discovery for him or her to review.

B. CJA and FDO Budgeting Concerns

Criminal Justice Act ("CJA") administrators, including the Court, which administers the CJA panel in many jurisdictions, and Federal Defender Organizations ("FDOs") (including both Federal Public Defender Organizations and Community Defender Organizations that provide indigent defense representation services), have an interest in avoiding the expenses incurred when an attorney or other member of the defense team must travel to lengthy legal visits merely to permit a detained client to review ESI on a defense team device. Subject to facility concerns discussed below, an investment in devices for use within a facility can result in substantial savings in this regard.

C. Court Concerns

The Court has an overriding interest in the delivery of e-discovery to detainees, among other reasons to avoid delays in cases resulting from the inability of detainees to access and review discovery necessary to participate in their defense. The Court also has an interest in minimizing discovery costs and discovery litigation and in avoiding collateral issues, such as motions for new counsel by detainees complaining about delays in reviewing discovery.

D. Facility Concerns

Constraints on detention facilities—the original bricks-and-mortar institutions—will probably pose the greatest challenges. These include most notably:

Personnel. The management of inmate movement, separation, and monitoring is personnel intensive and subject to strict scheduling. Maintaining and tracking devices and media; loading (and updating) discovery data; re-charging portable devices, etc., make intensive demands on IT personnel. But facilities may have little or no flexibility with available personnel.

Security. Weaponization of optical disk shards and other equipment, is a concern. Also, writable media may be used to pass messages to another inmate. Wireless and Internet capabilities have to be removed from devices used by detainees. (The BOP has a national policy against Internet and WiFi access for inmates.) Counsel (principally the Government) will need to screen ESI for disruptive contraband, such as pornography.

Sudden Change. Facilities' procedures can be changed to meet new needs. But attempts to suddenly impose new procedures to handle special circumstances may result in unintended breaches of standard security procedures, to potential great risk.

Space. It is optimal to allow inmates time and space to view their electronic discovery, and facilities should designate an area for discovery review. Consistent with the need to maintain security in a facility (to include, where appropriate, visual monitoring), efforts should be made to enable detainees to review their electronic discovery individually.

E. U.S. Marshals Service Concerns

At the national level, the USMS contracts with facilities to house pretrial detainees. At the local level, the USMS transports and safekeeps detainees. Transportation may be to and from court, or involve transferring a detainee from one facility to another. An occasionally used alternative to in-institution review of ESI is transporting inmates to locations that can accommodate discovery review. But that option has significant drawbacks of concern to the USMS. Specifically, given personnel and other restrictions, the Marshal has little capacity to transport detainees to, and safeguard detainees at, special facilities for the review of ESI. (In some jurisdictions, transportation time to and from the facility will render that impossible in any event.) Further, a detainee may not be placed in a facility that has superior ESI review resources if that facility does not fit the security designation of the detainee. For the USMS, providing a means of reviewing e-discovery within the detaining facility is optimal.

F. Government Concerns

The provision of e-discovery to detainees, although well under way in many districts, remains a process in development nationally. The Government's main concern is that the provision of e-discovery to detainees, which involves both technical challenges and new security challenges including unauthorized dissemination of discovery materials within and outside of the institution, should not be viewed as something the Government can make happen by pushing a digital button. Instead, these Guidelines reflect the multiple considerations that must be taken into account in preparing and providing ESI to detention facilities. In addition—it scarcely bears noting—different United States Attorney's Offices ("USAOs") have at this time varying capabilities to process and troubleshoot the production of e-discovery.

III. Practical Steps

A. Government, Defense, Facility and Judicial Points of Contact/Working Group

Points of Contact ("POCs") and a Working Group. Identifying POCs at the institutions listed below is our most important recommendation. Through informal meetings and direct dealings on individual cases POCs will develop an understanding of what devices are most readily acceptable to or available at a facility, what file formats are most readily reviewable by a detainee, and what particular obstacles may need to be addressed. The court should establish a Working Group, consisting at the least of judicial, CJA, FDO, DOJ, BOP, and U.S. Marshal representatives, to stimulate that process and to provide a forum for periodic reporting on developments and issuing useful local guidance.

USAO and facility POCs, as representatives of two government entities, will likely have the most frequent and direct communication. Ideally the contacts should include senior IT or litigation support specialists directly involved in the preparation and delivery, and receipt and mounting, of ESI for detainees. Within facilities, an appropriate POC may be someone involved in making the ESI available to inmates, such as unit managers or correctional counselors. There should also be USAO and facility POCs at the management level who can address policy issues and requests for exceptions (e.g., wardens, associate wardens, agency counsel).

A USMS POC can be helpful in arranging for POCs to be designated in contract facilities and in suggesting other methods for the delivery of ESI.

Public Defenders and their IT or litigation support specialists, and knowledgeable CJA attorneys, are likely to be productive POCs who can help other defense counsel in their jurisdiction. Defense POCs will be especially knowledgeable about exactly what electronic media the defense team may bring to a given facility for client review, the practical issues attendant thereto, and detainee experiences with the process.

Within the judiciary, CJA Supervisory Attorneys or other CJA administrators may have an overview of how discovery ESI has been handled, and can be cognizant of measures, such as the provision of laptops for a given case, that may engender substantial savings. Even more significantly, a judicial POC will be helpful in convening project status meetings, evaluating local CJA issues, and serving as a conduit for the expression of concerns to and from the court. As noted above, we specifically recommend that the court convene a Working Group to share issues, developments and solutions in the area.

On a national level, the following POCs may help with unique questions, or just getting an inmate e-discovery review program started: the Department of Justice's National Criminal Discovery Coordinator, Associate Deputy Attorney General Andrew Goldsmith (Andrew.Goldsmith@usdoj.gov); Criminal eDiscovery Coordinator John Haried (John.Haried@usdoj.gov); Associate U.S. Attorney (SDNY) John McEnany (John.McEnany@usdoj.gov); Administrative Office of the U.S. Courts National Litigation Support Administrator Sean Broderick (sean_broderick@fd.org); Federal Public Defender (Tampa, Florida) Donna Lee Elm (donna_elm@fd.org); Bureau of Prisons Assistant General Counsels Corinne Nastro (cnastro@bop.gov) and Monya Phillip (maphillip@bop.gov); U.S. Marshals Service Prisoner Operations Division's Heather Lowry (Heather.Lowry@usdoj.gov).

B. Identify Facility e-Discovery Capabilities

Recognizing that any inventory will be imperfect and subject to unexpected change, a working compilation by the POCs of the following information can be very useful:

a. How facilities allow detainees to review discovery: how do they determine who needs to review discovery; how much time do they typically provide detainees to review discovery; where do they allow detainees to review discovery (cell, law library, etc.); do detainees review discovery alone or in a group; if devices are used, do detainees share devices?

b. Facility devices: inventory facility equipment, broken out by pertinent inmate housing unit. This would include specifications of devices available; specification of installed software (including version); location of devices; number of devices; management of inmate access to devices; and hours of availability.

c. Facility Internet access, WiFi coverage, and policies, applicable both to detainees and to attorney visits.

d. Facility device limitations: e.g., hardware or other limits on installing specialized reviewing software; inability of facility devices to handle hardware-encrypted drives or

software-encrypted media; read/write restrictions (affecting not only a detainee's ability to tag items, but also a device's ability to handle viewing software that requires write-access to function).

e. Inmate-permitted media and devices: identify devices and media that the facility will generally accept for an inmate to use in a given case: e.g., CDs, DVDs, thumb drives, hard drives, .mp3 players, laptops.

    (i) Identify facility restrictions on devices for inmates: e.g., software restrictions (no games); hardware restrictions (no wireless); no built-in camera; no built-in microphone; no capability of connecting to an Ethernet network connection.

    (ii) See the comment on laptops under Special Responsibilities of Facilities.

f. The method that the facility uses to secure and inventory devices and storage media: the manner of storage, checkout, and checkin of storage media; and which personnel are trained and available to handle these tasks.

g. The methodology (if any) the facility can follow to update discovery provided on a rolling basis. For example, is the facility able and willing to use USAfx (a secure Dropbox-like file sharing platform) to accept ESI for inmates? (Note that supplementing, updating, or replacing storage media in a case where ESI has already been made available to a detainee may be difficult.)

h. Attorney devices: identify devices and media the facility will generally permit defense teams to bring for client visit, and practicalities attendant thereto.

C. Starting Up

Districts that are just beginning to consider provision of ESI to detainees may profitably begin considering: first, the types of ESI that are most voluminous and yet come in the most easily readable formats (such as wiretap intercepts in common audio formats and .pdfs of documents); second, the devices that the facilities have or will accept for review of that ESI; third, if devices need to be procured, how that will be done (e.g., by CJA funds for a given detainee in a given case); fourth, how procured devices will be configured for security and viewing; and fifth, how the devices will be loaded with ESI.

IV. Special Responsibilities of Participants

As noted above, this Guidance is not intended to create or define any legal rights. This section is intended only to articulate what we see as the practical division of labor in the collaborative venture of providing ESI to pretrial detainees.

A. Special Responsibilities of the Government

Early ESI Case Assessment. As an investigation begins and develops, an AUSA will have an increasingly refined idea of what types of ESI will be gathered, what platforms will be used to manage, review and produce the ESI; and which defendants may be detained in which facilities. Using available information and consulting with POCs as appropriate, the Government should identify anticipated e-discovery issues and prepare—even before arrest—a plan for speedy and

efficient provision of e-discovery to anticipated detainees. This will include ESI expected to be gathered at the time of arrest, such as cellphone data and other search warrant material. The Government will then be in a position to make a considered proposal to the defense and the court regarding provision of e-discovery. (For such planning purposes, we note again that rolling discovery may be difficult for facilities to manage.)

Provision of Trusted-Source and Screened Media. To provide assurance to the facility, ESI media and devices may have to be prepared (although not necessarily purchased) by the Government, and delivered by the Government to the facility. The Government should also screen out or redact material that may be disruptive to the institution (e.g., victim information, PII, CI information, obscene images, trade secrets, etc.) before production of the material to the pretrial detainee. (Screening out images such as cellphone pictures from an initial production of ESI to detainees may also substantially reduce the volume of data that needs to be produced.)

B. Special Responsibilities of the Defense

In keeping with the ESI Protocol, we anticipate that the defense will be a knowledgeable and constructive participant in discussions and meet-and-confers on this subject. In cases where difficulties derive from the volume of or unusual technical issues concerning ESI, the defense will prioritize what materials (whether select portions or all of the discovery) it provides to its client. Given software tools that can search and review voluminous discovery, the defense may be able to identify key documentation for the defendant's review.

In cases where the defense has selected key documentation for the defendant to review, it may be necessary for the defense to deliver the selected e-discovery to the facility and facility staff directly, without going through the government, in order to avoid revealing its work-product selection to the Government. The same may be true where the defense investigation has generated its own ESI. Some BOP facilities allow a defense attorney to mail in ESI directly to inmates via the special mail process upon submission of a form certification that the material on the media is in fact discovery related to the federal criminal proceeding and has not been altered in any way. Similar arrangements, perhaps endorsed by a court order, or involving a mutually trusted vendor, may be possible to satisfy security concerns at other facilities.

C. Special Responsibilities of the Court

The Court will consider the need of counsel and detainees to have adequate opportunity to review discovery in setting a trial schedule. Recognizing that the detention facility is not a party to the criminal litigation, and that both facility management and ESI discovery involve inherent limitations, the Court should generally afford the Government attorney an adequate opportunity to investigate and respond to asserted discovery review problems (including an opportunity to confer with facility and USMS representatives) before entering an order imposing specific procedures to govern the delivery and review of detainee ESI discovery. In cases presenting unusual technical or logistical issues, the court may also need to mediate the practical difficulties in providing discovery and the defendant's need to adequately assist counsel. Judicial participation in the Working Group referenced above will help judges stay abreast of developments in this area.

D. Special Responsibilities of the Facility

The facility must recognize its obligation to provide a reasonable opportunity for detainees to review ESI discovery. The need to provide ESI to detainees should be emphasized in USMS contracts with state, local and private facilities. Because laptops are inexpensive, have substantial storage, and can be configured to permit review of a wide variety of file formats, all USMS contract facilities should undertake to allow laptops as a routine method of providing ESI to detainees. (Many BOP facilities have standalone computers for inmate use that have been specially configured to handle most forms of e-discovery which should make consideration of laptops at BOP facilities unnecessary except in the most unusual of cases. Other BOP facilities have allowed the use of portable hard drives depending on the type of case and the volume of discovery.)

E. Special Responsibilities of the U.S. Marshals Service

At a national level, and with a view to eventually developing standards, the U.S. Marshals Service should begin to consider inmate e-discovery access in selecting and contracting with detention providers. At the local level the U.S. Marshals Service should, consistent with its resources and primary duties, assist in proposing solutions to e-discovery challenges.

V. Technical Considerations for the Non-Specialist

Obviously, most of those involved in the provision of ESI to detainees are not technology specialists. But following are some of the more technical points that non-technical personnel involved in the process will need to understand. The Technical Appendices contain other more detailed information gathered during preparation of these Guidelines that may also be useful for those approaching the subject.

A. Devices and Device Configuration

When a facility is willing to acquire, or to accept a laptop from the Government and/or the defense, either as part of its inventory,[5] or for a particular defendant in a particular case, the laptop will need to be configured to meet security concerns as well as to serve as an effective ESI review platform. The appendix contains suggested hardware specifications and application configurations that may provide a starting point in this regard. Facilities interested in obtaining their own ESI review devices may explore kiosks (housing for a publicly-used computer) designed specifically for the prison environment. (In 2016, kiosks priced at about $2200.)

MP3 players, iPods, DVD players, etc., can be inexpensive, Internet-free devices for reviewing common audio, video, and some document formats. However, smart phones and tablets (with WiFi and Internet capabilities) are largely pushing such media out of the market place. Note that it is not easy to modify devices to eliminate wireless capabilities, which may be required by a facility. Where iPads or other tablets do seem advisable, secure mounting of such devices may be an option to consider. *See, e.g.*, http://www.imageholders.com/collections/ipad-kiosks-tablet-enclosures-

[5] Note that the BOP, because of the anti-supplementation principle of federal appropriations, cannot itself take ownership of a device from an outside source.

wall-mounted; http://www.lilitab.com/blogs/news/13361673-the-ultimate-guide-to-configuring-your-ipad-for-kiosk-use.

As frequently discussed herein, portable hard drives are inexpensive and may be an excellent choice for producing ESI to facilities where detainees have access to computers.

B. Common File Types and Review Possibilities

General Viewers and Players. ESI discovery can involve an almost overwhelming number of potential file formats. The list of file formats (see the appendix) compiled by the BOP for its July 2014 RFI for inmate electronic discovery support services, hardware, and software is daunting. On the positive side, it is encouraging how many file formats commercial viewers and players can support. By way of example, the files supported by Quick View Plus 13 Professional, and Windows Media Player 12, are also listed in the appendix.

Forensic Image Viewers. Seized media is often forensically imaged via AccessData's Forensic Toolkit® (FTK®) or Guidance Software's EnCase Forensic, both of which provide viewers that can be loaded onto a laptop to view forensic images contained in an attached hard drive. These viewers are not very simple to use, and it may be most effective to provide extracted user files. Extracted files may also be necessary where the underlying forensic image contains inappropriate material, such as pornography or hacker tools.

Native or Proprietary Formats. The extent to which user files must be viewable via native software; the existence of files in proprietary format; the significance of hyperlinks; and other matters not here imagined, will create additional issues. Application of this Guidance and of the 2012 JET-WG Recommendations will assist in bringing things down to manageable elements.

Litigation Support Databases. Databases such as Concordance, iPRO Eclipse SE, and Relativity (all commonly used by the Government) as well as CaseMap and Summation (commonly used by the Defense) may present a greater level of complexity. Concordance and iPRO Eclipse SE are desktop-based and can (subject to volume) be loaded onto a laptop. Relativity can export data for use on standalone devices. If an Internet (remote access)-based platform is used, the ability to export relevant portions to a laptop- or iPad-viewable format will have to be considered.

Read-Write Access. Some review platforms and programs, such as video players, require read-write access to the computer to function, for example to write .tmp files. This may require workarounds when write access to devices available to detainees is restricted.

Note-Taking by Detainees. Because many facilities, including BOP facilities, will not allow users write-access to discovery review devices for security and device-maintenance reasons, detainees will not be able to flag or tag documents electronically. Counsel should anticipate developing paper-based charts or forms that will facilitate flagging items of interest.

Remote (Web- or Cloud-Based) Data. Although data and electronic devices are increasingly configured to store and access data and software remotely—in the cloud—limitations or prohibitions on Internet access within facilities will largely preclude their use in providing e-discovery to detainees, at least in the foreseeable future. Accordingly, in selecting platforms for

attorney review, the ability to download data to standalone devices in a useable format for detainee review will remain key.

C. Encryption

In all instances a determination must be made whether the ESI can be produced in encrypted format (the Government default) and still be effectively reviewed; whether encrypted hard drives (e.g. Addonics) will be suitable; or whether data must be produced in unencrypted format, and any additional security measures that may entail.

Technical Appendices

I. Identification of Installed Software

A useful tool for the identification of software (and version) installed on a facility computer may be the Windows Management Instrumentation Command, e.g., running **`wmic product list brief`** at the command line.

II. E-Discovery Review Laptop Configuration Suggestions

A. General Suggestions

Where laptops are available for ESI review, following are some configuration suggestions:

- Hardware modifications—remove or disable
  - RJ-45 network jack for standard network cable
  - Wi-Fi cards/antennas. (Even if there is no WiFi in the facility, someone could possibly smuggle in a WiFi hotspot.
  - Phone modems (usually found only on older equipment).

- Processing and storage specifications
  - Processor: 1 gigahertz (GHz) or faster.
  - RAM: 1 gigabyte (GB) (32-bit) or 2 GB (64-bit)
  - Minimum Hard Drive Size: 250+GB, or even a partitioned drive with 500 GB D: drive.
  - Graphics card: Microsoft DirectX 9 graphics device with WDDM driver

- Operating System
  - Windows 10, which will soon be the standard in many federal agencies, and will not soon need to be upgraded.
    - Contains Windows Media Player (verify)

- Security Software, to reduce the possibilities for unauthorized use and to reset the laptop during reboot to its previous-state configuration, as set by the administrator.

  - Lockdown software, to inhibit users from making changes. For example,
    -Mirabyte http://www.mirabyte.com/en/products/frontface-lockdown-tool/features.html
    -Inteset Systems http://shop.inteset.com/lock-down-windows-with-inteset-secure-lockdown

  - Restore software, to reset the laptop during reboot to its previous-state configuration. For example:
    -Deep Freeze, http://www.faronics.com/products/deep-freeze/enterprise/
    -Reboot Restore RX (free, but additional testing required): http://www.horizondatasys.com/en/products_and_solutions.aspx?ProductId=18#Benefits

- Reviewing Software
    - Eclipse SE Data format. Where the Government has ESI in Eclipse SE format, the Government is licensed to use Eclipse Publish to create a stand-alone version of selected data to load onto a laptop. Commencing in summer 2016, the Government has been licensed to make Oracle's Outside In Viewer (which is used in Eclipse) available for viewing databases created via Eclipse Publish. The Outside In Viewer can handle hundreds of file formats, similar to Quick View Plus, whose supported file formats are listed below.
    - Custom video surveillance software, where it is easier to install a custom program, rather than to convert non-standard video files into a format viewable by standard Windows Media Player.
    - (This list is expected to change and grow.)

B. BOP July 2015 Specifications

For information only, to help guide thinking, the following is taken from BOP's February 2015 specifications for detainee discovery viewing devices inside BOP facilities:

1. Operating System and Software Security Features

a. Operating system

Windows 7 Professional

b. Third-Party Software

Romaco Timer (Free Commercial) is a utility used to set a time limit on the user usage. It is currently set to logoff the current user in two hours. Prior to being logged out the user will receive a prompt indicating that they have five minutes remaining before the system automatically logs them off. This mechanism was put in place to ensure that the needs of a large inmate population; needing the use of discovery workstations with a limited supply, are met. If no other inmate needs to use the workstation, a given inmate can log back in and use it. A new Timer created in Visual Basic (VB) may replace the Romaco Timer and help support future operating systems.

Reboot RX Free takes a snapshot of the pc environment.

Quick View Plus 12 (BOP Licensed) is a file viewer for a variety of different file formats.

VLC Player (Free Commercial) is a media player for playing a variety of different media formats not supported by Windows Media Player.

For The Record (FTR) software to support proprietary video.

2. Security Features

The security/lockdown of the e-discovery pc comes from Group Policies built into Windows 7. A Local Group Policy was created that is assigned to the "Users" group.[6] The policy is located in in the C:\Windows\system32\GroupPolicyUsers\ folder. Security features configured in the LGPO (Local Group Policy Object) for the inmate environment are:

- The C:\ drive is not visible to the user under Windows Explorer
- Disabled the use of programs that could be used to generate scripts and environment configuration changes such as Control Panel, cmd.exe, powershell.exe, notepad.exe, taskmanager.exe etc.
- Disabled writing to USB drives
- Disabled writing to CDR's
- Desktop right click disabled
- CTRL+ALT+DEL does not display any options such as Task Manager.
- Start Menu only shows "Log Off" option. "Log Off" option is tied to a batch file that forces the system to restart. This forces the system back to the original snapshot of the system in Reboot Restore RX.
- Profile folders such as My Documents, Picture, and Video etc. are accessible to the user. They can write to these locations. This helps support encrypted files that need to be extracted and written to the local drive.
- Desktop icons available are the My Computer, VLC Player, Windows Media Player, Quick View Plus 12 icons
- Drives available in the user environment are the local CDROM drive and any USB external drives plugged into the system.
- Added a visual security feature. Two distinct wallpapers were created to specify whether the current environment is a "Users" or an "Administrator". This will ensure the inmate is logged into the appropriate locked down environment.

[6] BOP's detailed list of Windows GPO settings is not reproduced here.

III. Common File Types and Review Applications

A. File Types Listed in the BOP July 2014 Electronic Discovery RFI

The following is taken from the July 7, 2014, BOP RFI for support services, hardware and software for inmate electronic discovery.,
https://www.fbo.gov/index?s=opportunity&mode=form&id=fa1f57c38041cf651e1297aeb33f295c&tab=core&_cview=1

The following introduction to the BOP RFI is a useful presentation of BOP thought and restrictions in this area.

> The Federal Bureau of Prisons (BOP), Information Technology Planning and Development Branch has created a Request for Information to seek information related to support services, hardware, and software for inmate electronic discovery (eDiscovery). The goal of this RFI is to obtain detailed information for a secure computing device which can be used by inmates to view discovery materials related to their criminal defense against federal prosecution or their civil litigation against a federal entity. The BOP seeks information on available solutions for an eDiscovery system that incorporates actual hardware, any necessary software to view litigation material, and support services for BOP IT staff to troubleshoot issues or seek repair of equipment. Interested parties shall not be reimbursed for any costs related to the development and submission of information in response to this RFI.
> . . . .
> These will be stand-alone read-only devices used to view as many different types of data as possible. The device should have the ability to receive updates to read additional types of data as needed. The task of updating the devices to include more capabilities could be done by the vendor or the vendor could provide a simple update for local staff to perform. These devices WILL NOT have internet connectivity.

Word Processing Formats
Adobe FrameMaker (MIF) 6.0, text only
Corel WordPerfect for Windows through X4
Lotus WordPro 96 – Millennium Edition 9.6, text only
Lotus Symphony Documents 1.2
Microsoft Windows Works through 4.0
Microsoft Word for Windows and Mac through 2010
Microsoft WordPad
Open Office Writer 2.0, 3.0
StarOffice Writer 5.2 - 9
ANSI Text 7 & 8 bit
ASCII Text 7 & 8 bit
EBCDIC all
HTML through 3.0
IBM Revisable Form Text all
Microsoft Rich Text Format (RTF)
Unicode Text all
WML 1.2
XML
MacWrite II 1.1
DOS Word Processors
DisplayWrite 2 & 3 (TXT) all
DisplayWrite 4 & 5 through Release 2.0
Professional Write through 2.1

Spreadsheet Formats
Corel QuattroPro for Windows through X4
Lotus 1-2-3 (DOS & Windows) through 5.0
Lotus 1-2-3 (OS/2) through 2.0
Lotus 1-2-3 for SmartSuite 97 – Millennium Edition 9.6
Lotus Symphony 1.0, 1.1 and 2.0

Microsoft Excel for Windows or Mac through 2010
Microsoft Works through 4.0
OpenOffice Calc 2.0 and 3
StarOffice Calc 5.2, 6.x, 7.x - 9

Database Formats
Access through 2010
dBASE through 5.0
Microsoft Works through 4.0

Presentation Formats
Corel Presentations 3.0 – X4
Harvard Graphics for Windows
Lotus Symphony Presentations 1.2
Microsoft PowerPoint through 2010
OpenOffice Impress 1.1 - 3
StarOffice Impress 6 – 9

Graphic Formats
Adobe Acrobat (PDF) 6.0 – 10.0
Adobe Illustrator 7.0, 9.0
AutoCad Interchange & Native Drawing Formats (DXF & DWG) 2.5 – 2.6, 9.0 – 14.0, 2000i, 2002, 2005 - 2010
Bitmap (BMP, RLE, ICO, CUR, OS/2 DIB & WARP) all
Corel Clipart (CMX) 5 – 6
Corel Draw (CDR) 6.0 – 8.0
Corel Draw (CDR with TIFF header) 2.0 – 9.0
DCX (multipage PCX) Microsoft Fax
Encapsulated PostScript (EPS) TIFF header only
Graphics Interchange Format (GIF)
Hewlett Packard Graphics Language (HPGL) 2
JPEG all
MacPaint (PNTG)
OpenOffice Draw 3
Portable Network Graphics (PNG) 1.0
Star Office Draw 9
TIFF through 6
TIFF CCITT Group 3 & 4 through 6
WordPerfect Graphics 7 and 10 (WPG & WPG2)

Video Formats
MPEG-1/2
DIVX (1/2/3)
MPEG-4 ASP, DivX 4/5/6, XviD, 3ivX D4
H.263 / H.263i
H.264 / MPEG-4 AVC
Cinepak
Theora
MJPEG (A/B)
WMV-9 / VC-1 1
Quicktime
DV (Digital Video)
Indeo Video 4/5 (IV41, IV51)
Real Video ¾

Audio Formats
MPEG Layer 1/2
MP3 (MPEG Layer 3)
AAC - MPEG-4 part3
Vorbis
WMA 1/2
WMA 3 1
FLAC
ATRAC 3
Wavpack
APE (Monkey Audio)
Real Audio 2
AMR (3GPP)
MIDI 3
DV Audio
QDM2/QDMC (QuickTime)

B. Quick View Plus 13 Professional, Supported File Formats

This gives an idea of the variety of file formats one commercially available viewing platform can present. See Quick View Plus 13 Professional, Fact Sheet and Supported File Formats, available at http://avantstar.com/metro/reference?path=A1x478ex1y1x4794x1x66y1x4a6fx1x65y8x656bx8x1.

WORD PROCESSING VERSIONS

GENERIC TEXT
ANSI Text—7 & 8 bit
ASCII Text—7 & 8 bit
EBCDIC—all
HTML—through 3.0 (with limitations)
IBM FFT—all
IBM Revisable Form Text—all
Microsoft Rich Text Format (RTF) —all
Trillian text
Unicode Text —all
WML —1.2
XML

DOS WORD PROCESSORS
DEC WPS Plus (DX)—through 4.0
DEC WPS Plus (WPL)—through 4.1
DisplayWrite 2 & 3 (TXT)—all
DisplayWrite 4 & 5—through Release 2.0
Enable—3.0, 4.0 and 4.5
First Choice—through 3.0
Framework—3.0
IBM Writing Assistant—1.01
Lotus Manuscript—2.0
MASS11—through 8.0
Microsoft Word—through 6.0
Microsoft Works—through 2.0
MultiMate—through 4.0
Navy DIF—all
Nota Bene—3.0
Office Writer—4.0 – 6.0
PC-File Letter—through 5.0
PC-File+ Letter—through 3.0
PFS:Write—A, B and C
Professional Write—through 2.1
Q&A —2.0
Samna Word—through Samna Word IV+
SmartWare II—1.02
Sprint—through 1.0
Total Word—1.2
Volkswriter 3 & 4—through 1.0
Wang PC (IWP)—through 2.6
WordMARC—through Composer Plus
WordPerfect—through 6.1
WordStar—through 7.0
WordStar 2000—through 3.0
XyWrite—through III Plus

WINDOWS WORD PROCESSORS
Adobe FrameMaker (MIF)—6.0, text only
AMI/AMI Professional—through 3.1
Corel/Novell WordPerfect
for Windows—through X5
Hangul—97, 2002, 2010
JustSystems Ichitaro
—5.0, 6.0, 8.0 – 13.0, 2004, 2010
JustWrite —through 3.0
Kingsoft WPS Office Writer—2010
Legacy —through 1.1
Lotus WordPro
—96 – Millennium Edition 9.6, 9.8 (text only)
Lotus Symphony Documents—1.2
Microsoft Windows Works—through 4.0
Microsoft Windows Write—through 3.0
Microsoft Word for Windows—through 2013
Microsoft WordPad—all
Novell Perfect Works—2.0
OpenOffice Writer—1.1 – 3.0
Oracle Open Office Writer—3.0
Professional Write Plus—1.0
Q&A Write for Windows—3.0
StarOffice Writer—5.2 – 9.0
WordStar for Windows—1.0

MACINTOSH WORD PROCESSORS
MacWrite II—1.1
Microsoft Word
—3.0, 4.0, 98, 2001, v.X, 2004, 2008
Microsoft Works—through 2.0
Novell WordPerfect—1.02 – 3.0

SPREADSHEETS VERSIONS
Corel QuattroPro for Windows
—through X5
Enable—3.0, 4.0 and 4.5
First Choice—through 3.0
Framework—3.0
KingSoft WPS Office Spreadsheet—2010
Lotus 1-2-3 (DOS & Windows)—through 5.0
Lotus 1-2-3 Charts (DOS & Windows)
—through 5.0
Lotus 1-2-3 (OS/2) —through 2.0
Lotus 1-2-3 Charts (OS/2)—through 2.0
Lotus 1-2-3 for SmartSuite
—97 – Millennium Edition 9.6, 9.8
Lotus Symphony—1.0 – 1.2 & 2.0
Microsoft Excel Charts—2.x – 7.0
Microsoft Excel for Macintosh
—3.0 – 4.0, 98, 2001, v.X, 2004, 2008
Microsoft Excel for Windows
—2.2 through 2013
Microsoft Multiplan—4.0
Microsoft Windows Works—through 4.0
Microsoft Works (DOS)—through 2.0
Microsoft Works (Mac)—through 2.0
Mosaic Twin—2.5
Novell Perfect Works—2.0
OpenOffice Calc—1.1, 2.0 (text only), 3.0
Oracle Open Office Calc—3.0
Quattro Pro for DOS—through 5.0
PFS:Professional Plan—1.0
SmartWare II—1.02
StarOffice Calc—5.2, 6.x, 7.x, – 9.0
SuperCalc 5—4.0
VP Planner 3D—1.0

DATABASES VERSIONS
Access—through 2.0, 95-2000
dBASE—through 5.0
DataEase—4.x
dBXL—1.3
Enable—3.0, 4.0 and 4.5
First Choice—through 3.0
FoxBase—2.1
Framework—3.0
Microsoft Windows Works—through 4.0
Microsoft Works (DOS)—through 2.0
Microsoft Works (Mac)—through 2.0
Paradox (DOS)—through 4.0
Paradox (Windows)—through 1.0

Personal R:BASE—1.0
Q & A—through 2.0
R:BASE 5000—through 3.1
R:BASE System V—1.0
Reflex—2.0
SmartWare II—1.02

PRESENTATIONS VERSIONS
Corel/Novell Presentations—3.0 – X5
Freelance for Windows
—through Millennium Edition 9.6, 9.8
Freelance for OS/2—through 2.0
Harvard Graphics for DOS—2.x & 3.x
Harvard Graphics for Windows
KingSoft WPS Office Presentation—2010
Lotus Symphony Presentations—1.2
Microsoft PowerPoint for Macintosh
—3.0 – 4.0, 98, 2001, v.X, 2004, 2008
Microsoft PowerPoint for Windows
—3.0 through 2013
OpenOffice Impress—1.1 – 3.0
Oracle Open Office Impress—3.0
StarOffice Impress —5.2 (text only), 6.0 – 9.0

COMPRESSED VERSIONS
7z
GZIP
JAR
LZA Self Extracting Compress
LZH Compress
Microsoft Binder—7.0 – 97
MIME (Text Mail)
RAR
UNIX Compress
UNIX TAR
UUEncode
ZIP—PKWare through 2.04g

OTHER VERSIONS
Apple iWork 09 Keynote
Apple iWork 09 Numbers
Apple iWork 09 Pages
Executable (EXE, DLL)
Executable for Windows NT

Lotus Notes DXL
Microsoft Outlook
Express (EML)—97 – 2003
MBOX
Microsoft Cabinet
Microsoft Live Messenger—10
Microsoft Office 2003 XML (text only)
Microsoft OneNote 2007-2010 (text only)
Microsoft Outlook Folder (PST)—97 – 2003
Microsoft Outlook Forms Template (OFT)
Microsoft Outlook Offline Folder (OST)
—97 – 2003
Microsoft Outlook Message (MSG)
Microsoft Project—98, 2000, 2002,
2003, 2007, 2010 (Gantt chart view)
vCard—2.1

GRAPHIC VERSIONS

Adobe Acrobat (PDF)—2.1, 3.0 – X
Adobe PDF Package
Adobe PDF Portfolio
Apple Mail Message—2.0
Adobe Illustrator—7.0, 9.0, CS5, CS6
Adobe Photoshop (PSD)—4.0, CS5, CS6
AmiDraw (SDW)—all
AutoCad Interchange & Native
Drawing Formats (DXF & DWG)
—2.5 – 2.6, 9.0 – 14.0, 2000i,
2002, 2005 – 2012
Autoshade Rendering (RND)—2.0
Binary Group 3 Fax
—‘2005 - 2007 (with limitations)
Bitmap (BMP, RLE, ICO,
CUR, OS/2 DIB & WARP)—all
CALS Raster—Type I and Type II
Computer Graphics Metafile (CGM)
—ANSI, CALS NIST 3.0
Corel Clipart (CMX)—5 – 6
Corel Draw (CDR)—6.0 – 8.0
Corel Draw (CDR with TIFF header)
—2.0 – 9.0
DCX (multipage PCX)—Microsoft Fax
GEM Paint (IMG)
Graphics Interchange Format (GIF)
Hewlett Packard
Graphics Language (HPGL)—2
JFIF (JPEG not in TIFF format)—all
JPEG—all
Kodak Flash Pix (FPX)—all
Kodak Photo CD (PCD)—1.0
Lotus 1-2-3 Picture File Format (PIC)—all
Lotus Snapshot—all
Macintosh PICT1 & 2—Bitmap only
MacPaint (PNTG)
Micrografx Draw (DRW)—through 4
Micrografx Designer (DSF)—Windows 95,
6.0
Novell PerfectWorks (Draw)—2.0
OpenOffice Draw—3.0
Oracle Open Office Draw—3.0
Paint Shop Pro (PSP)—5.0 – 7.04
PC Paintbrush (PCX & DCX)—all
Portable Bitmap (PBM)
Portable Graymap (PGM)
Portable Network Graphics (PNG)—1.0
Portable Pixmap (PPM)
Progressive JPEG
Star Office Draw—9.0
Sun Raster (SRS)
SVG (XML display only. Content will be
rendered as an XML file, not a multimedia
file.)
TIFF—through 6
TIFF CCITT Group 3 & 4—through 6
Truevision TGA (TARGA)—2
Visio—4 (preview only), 5, 2000, 2002,
2003
WBMP
Windows Enhanced Metafile (EMF)
Windows Metafile (WMF)
WordPerfect Graphics
—through 2.0, 7 and 10 (WPG & WPG2)
X-Windows Bitmap (XBM)—x10
compatible
X-Windows Dump (XDM)—x10
compatible
X-Windows Pixmap (XPM)—x10
compatible

C. Windows Media Player 12

Following is a list of audio and video files supported by Windows Media Player 12. *See* https://support.microsoft.com/en-us/kb/316992

Windows Media formats (.asf, .wma, .wmv, .wm)
Windows Media Metafiles (.asx, .wax, .wvx, .wmx)
Windows Media Metafiles (.wpl)
Microsoft Digital Video Recording (.dvr-ms)
Windows Media Download Package (.wmd)
Audio Visual Interleave (.avi)
Moving Pictures Experts Group (.mpg, .mpeg, .m1v, .mp2, .mp3, .mpa, .mpe, .m3u)
Musical Instrument Digital Interface (.mid, .midi, .rmi)
Audio Interchange File Format (.aif, .aifc, .aiff)
Sun Microsystems and NeXT (.au, .snd)
Audio for Windows (.wav)
CD Audio Track (.cda)
Indeo Video Technology (.ivf)
Windows Media Player Skins (.wmz, .wms)
QuickTime Movie file (.mov)
MP4 Audio file (.m4a)
MP4 Video file (.mp4, .m4v, .mp4v, .3g2, .3gp2, .3gp, .3gpp)
Windows audio file (.aac, .adt, .adts)
MPEG-2 TS Video file (.m2ts)

D. Litigation Support Database Applications

Concordance
iPRO
iPRO Eclipse SE
Relativity
Access Data – Summation
Intella
Nuix
Epiq
CaseLogistics
Masterfile
iConnect
Lateral Data

* * *