EOUSA RIP

U.S. Department of Justice

Executive Office for United States Attorneys

Office of the Director

Room 2261, RFK Main Justice Building
950 Pennsylvania Avenue, NW
Washington, DC 20530

(202) 514-2121

MEMORANDUM - Sent via Electronic Mail

DATE: May 4, 2009

TO: ALL UNITED STATES ATTORNEYS
ALL FIRST ASSISTANT UNITED STATES ATTORNEYS
ALL CRIMINAL CHIEFS
ALL CIVIL CHIEFS

/s/
FROM: H. Marshall Jarrett
Director

SUBJECT: Prisoner E-Mail Accounts

ACTION REQUIRED: Use voluntary requests, not subpoenas, when seeking BOP prisoner email communications.

CONTACT PERSONS: [redacted]
Assistant United States Attorney
Legal Initiatives Staff
EOUSA
Telephone: (202) [redacted]
E-mail: [redacted]@usdoj.gov

[redacted]
Assistant United States Attorney
Eastern District of Pennsylvania
Telephone: (215) [redacted]
E-mail: [redacted]@usdoj.gov

The Bureau of Prisons (BOP) has begun to offer prisoners at some institutions access to email accounts. Your offices will, on occasion, need to see the contents of such prisoner email communications to successfully prosecute your cases. This memorandum provides notice that the best method of obtaining the content of BOP prisoner email accounts is simply to write to the warden at the prison or detention center in question, asking BOP to voluntarily provide the contents of the emails. This procedure is unlike what you may be using to obtain prisoner telephone records or letters, which typically are, and will continue to be, obtained via legal

process. However, using a subpoena to obtain prisoner email communications may, in some circumstances, cause a prisoner to file an unwarranted civil action against the United States or an individual Assistant United States Attorney (AUSA).

Under 18 U.S.C. § 2703(b), the Stored Communications Act, when a government entity requires the disclosure of the contents of an email communication, notice must be given to the email customer, i.e., the prisoner, in certain circumstances. Thus, were an AUSA to send the BOP a grand jury subpoena seeking these records, and were a BOP employee to produce the information without notifying the prisoner, such conduct could in some circumstances subject the AUSA to a prisoner lawsuit under 18 U.S.C. § 2707. That section provides a civil cause of action against persons who violate the terms of the Stored Communications Act. Although a variety of strong defenses would be available to defend such an action, you should avoid the risk of any such lawsuit by simply asking BOP to voluntarily produce prisoner emails.

According to its own policy, the BOP does not require a subpoena to provide you with the contents of prisoner email communications. BOP's policy on the prisoner email system is attached. Page eight of the policy authorizes BOP to provide copies of the emails without a subpoena. The BOP does not provide notice to the prisoner of your request for the production of email communications. A suggested form letter to use when requesting prisoner email communications is attached. Although BOP policy requires that BOP retain prisoner email communications for six months, current BOP practice is to retain them for a longer period of time. In addition, upon specific request, the BOP will retain specific emails indefinitely.

Currently, the following BOP prisons and detention centers have operational prisoner email accounts systems: Alderson, Allenwood Complex, Bryan, Carswell, Coleman, Camp and Low, Cumberland, Danbury, Devens, Fairton, Hazelton, Herlong, Honolulu, Jesup, Marion, Marianna, Miami FCI, Montgomery, Morgantown, Otisville, Pensacola, Philadelphia, SeaTac, Sheridan, Terre Haute - CMU only, Terminal Island, Texarkana, Three Rivers, and Victorville Complex. BOP indicates that by December 2010, it expects that all sites in the BOP system will have operational email accounts available.

Please also note that page three of the attached BOP policy discusses the criteria by which certain prisoners are excluded from having access to the BOP email account system.

Questions about the practical aspects of obtaining prisoner emails may be directed to [redacted] at the contact information above. Questions regarding the Stored Communications Act may be directed to AUSA [redacted] at the contact information above, or to [redacted] Associate Director, Office of Enforcement Operations, at (202) [redacted] or the Computer Crime and Intellectual Property Section, at (202) [redacted]

cc: ALL UNITED STATES ATTORNEY'S SECRETARIES
Attachments

Chapter 14. TRUST FUND LIMITED INMATE COMPUTER SYSTEM

14.1 GENERAL

The Trust Fund Limited Inmate Computer System (TRULINCS) provides inmates with a computer system that does not jeopardize the safety, security, orderly operation of the correctional facility, or the protection of the public or staff. Inmates participating in the program must accept rules identified in the TRULINCS Electronic Messaging Warning/Responsibility/ Acknowledgment Statement prior to accessing the system. Inmates do not have access to the Internet.

14.2 AUTHORITY

The Bureau's authority to operate TRULINCS is found in 18 U.S.C. 4042, which authorizes the Bureau to provide for the safekeeping, care, and subsistence of Federal prisoners. Pursuant to that authority, the CEO prohibits or discontinues its operation, or individual inmate's participation, whenever it is determined to jeopardize the safety, security, or orderly operation of the correctional facility, or the protection of the public and staff.

Use of TRULINCS is a privilege; therefore, the Warden may limit or deny the privilege of a particular inmate (see Section 14.9 for restrictions). This authority may not be delegated below the Associate Warden level.

Individual inmates may be excluded from program participation or individual services as part of classification procedures (see Section 14.9). Information supporting the exclusion is forwarded to the Warden for final determination.

14.3 RESPONSIBILITIES

a. **TRULINCS Coordinator.** The Chief of the Trust Fund Branch is the designated TRULINCS Coordinator – the resource person for Bureau staff, other components of the Department of Justice, law enforcement agencies, and the general public.

b. **Trust Fund Supervisor.** The Trust Fund Supervisor has responsibility for the overall operation of TRULINCS at the institution. The Trust Fund Supervisor administers, maintains, and monitors the system; provides training to inmates during Admission and Orientation; supervises inmate workers assigned to the TRULINCS detail; and responds to inmate inquiries regarding the system.

The Trust Fund Supervisor is also the designated System Supervisor and maintains internal controls, system integrity, user accounts, and all other aspects of TRULINCS security and operations.

c. **Staff Use.** Staff members may not use TRULINCS for personal use.

d. **Contacts and Inmates.** By participating in the TRULINCS Program, inmates, and the contact(s) with whom they correspond, voluntarily consent to having all email, including transactional data, and system activity, monitored and retained by authorized personnel. This authority includes rejecting individual emails sent to or from inmates that jeopardize the above-mentioned interests.

(1) An inmate's participation in the TRULINCS Program is conditioned on their notice, acknowledgment, and voluntary consent to the Warden's authority, as indicated above. Inmates consent to monitoring when they accept the TRULINCS Electronic Messaging Warning/Responsibility/Acknowledgment Statement each time they access the system.

(2) A community person's consent to Bureau staff monitoring of all TRULINCS emails and activity is obtained when the person receives the initial system-generated email notifying him/her the inmate wants to add him/her to their contact list and when he/she proceeds with corresponding.

14.4 RATES

The Chief of the Trust Fund Branch, with the concurrence of the Assistant Director of the Administration Division, sets all program fees. By participating in the program, the inmate consents to have the Bureau withdraw program fees directly from their Deposit Fund account.

14.5 EQUIPMENT AND SUPPLIES

a. **Equipment.** Inmate computers and printers must clearly display a blue label as "INMATE ACCESS."

Requests for additional equipment are forwarded from the Warden through the Regional Trust Fund Administrator to the Chief of the Trust Fund Branch for consideration.

b. **Multi-Purpose Workstations.** Ordinarily, workstations are located in the housing units and law library. Requests for alternative locations are forwarded from the Warden through the Regional Trust Fund Administrator to the Chief of the Trust Fund Branch for consideration.

Workstations located in the housing units ordinarily are multi-purpose, offering various services with the exception of the Electronic Law Library (ELL) and Print Services. Workstations located in the institution Law Library ordinarily offer access to only the ELL Service and limited supporting services (e.g., TRU-Unit Management and Bulletin Board Services). TRULINCS ELL workstations are located in the Law Library due to the sensitivity of information and supervision within the area.

c. **Print Stations.** Ordinarily each institution will have two print stations available on the main compound and one in a satellite camp. Requests for additional locations are forwarded from the

Warden through the Regional Trust Fund Administrator to the Chief of the Trust Fund Branch for consideration.

d. **Operating Supplies.** Funds are provided in the annual TRULINCS budget to purchase operating supplies (e.g., paper, toner, mailing labels). Procedures for procuring these items are in Chapter 2.

14.6 TRULINCS INMATE WORKERS

Inmates receive compensation from the Trust Fund Appropriation for work performed in support of TRULINCS. Relatively short absences due to callouts, hospitalization, sick line, etc., do not affect the period covered. Extended absences such as furloughs, lay-in assignments, or lockdowns are not compensable.

a. **Screening of Inmate Workers.** Inmates who refuse to participate in the Inmate Financial Responsibility Program may not work in TRULINCS. Prior to assigning inmates to the detail, the Trust Fund Supervisor shall request the Special Investigative Supervisor (SIS) to determine if any issues exist that raise security concerns (e.g., ongoing investigation).

b. **Work Hours.** Ordinarily, TRULINCS inmate work details do not exceed four hours per day. Institutions may determine the appropriate work hours based on availability of funds provided in the annual budget.

c. **Rate of Pay.** The hourly rate of pay for inmates assigned to TRULINCS activities is:

$0.55 per hour starting
$0.75 per hour after 3 months' service, if warranted

Any increase in pay (not to exceed $0.75 per hour) is based on the inmate's work performance and availability of funds provided in the annual budget.

d. **Bonus Pay.** Bonus Pay may be awarded to TRULINCS inmate workers. It may not exceed one-half of the inmate's monthly pay. A bonus recommendation is made by the work assignment supervisor.

e. **Restrictions on Inmate Duties.** TRULINCS equipment should be secured adequately to prevent inmates from accessing the internal components of computers or peripherals. If inmates are used to clean secured equipment (e.g., workstations, printers), they must be directly supervised by staff at all times to prevent theft, damage, or misuse, until the equipment is secured.

14.7 ACCOUNTING

a. **Daily Reconciliation.** Staff responsible for Deposit Fund accounting compare the TRUFACS Withdrawal Report total (TRUFACS Withdrawal Type = TRUL Withdrawal) with the

TRULINCS Reconciliation with TRUFACS Report daily. Staff verify that these balances are equal. If they differ, staff contact the Central Office Trust Fund Branch Deposit Fund immediately. Upon verification of the balances, the Deposit Fund staff member uploads the daily TRULINCS extract to the automated accounting system.

b. **Monthly Reconciliation.** Staff complete the monthly reconciliation as required in the institution proof-check.

c. **Refunds.** Refunds are provided in the following circumstances:

- When granted by the Trust Fund Supervisor as a result of a system malfunction that has been documented through the trouble ticket system.
- Refunds for printer malfunctions, in the form of a reprint unless documented through the trouble ticket system.
- When granted by the Central Office when purchased media has been deemed defective, explicit, or inappropriate.

d. **Funds Returned to TRUFACS.** Funds are returned to TRUFACS by staff only in the following circumstances:

- Inmates are released.
- Inmates on Public Messaging and/or MP3/Music restriction for more than 60 days may request in writing that their TRU-Units be returned to their Commissary account. This is a one-time transaction for the entire TRU-Unit balance.
- In rare or unusual instances deemed appropriate by the Warden when inmates do not have access to TRULINCS. In these circumstances, Trust Fund staff are given written documentation to support the transfer. This is a one-time transaction for the entire balance.

e. **Processing Inmate Releases.** A TRULINCS account is released when an inmate is released in TRUFACS. If there is a communication issue between TRUFACS and TRULINCS, staff may proceed with the release in TRUFACS. A secondary TRUFACS release to transfer the inmate's TRU-Units must be completed once connection with TRULINCS is restored. The Trust Fund Specialist shall run the TRULINCS Released Inmate with TRU-Unit Balance Report weekly and take corrective action for inmates listed on this report.

14.8 INMATE ACCOUNTS. TRULINCS inmate accounts are established and maintained automatically through the TRUFACS nightly process.

a. **Account Access.** Inmates access their accounts using their eight-digit register number; nine-digit phone access code (PAC); and fingerprint identification or four-digit Commissary personal identification number (PIN).

It is the inmate's responsibility to maintain possession of his/her login information. Inmates will not disclose passwords (login criteria) to anyone and will log off the system when leaving the

TRULINCS terminal.

b. **Locked Accounts.** After three consecutive failed attempts to access the system, the inmate's account is locked. Inmates request in writing to the Trust Fund Supervisor that their accounts be unlocked.

14.9 SYSTEM ACCESS

It is important that staff ensure inmates are only restricted from using TRULINCS, or individual TRULINCS services, when absolutely necessary to protect the safety, security, or orderly operation of the correctional facility, or the protection of the public or staff.

Due to the "self-service" format TRULINCS provides, all inmates who are physically capable of accessing a TRULINCS terminal should be provided access in all but limited cases. Public Messaging is the only exception to this approach, as it involves communication with persons in the community and the possibility of continuing criminal or other prohibited activity that may jeopardize the safety and security of the institution.

a. **Program/Service Exclusions.** Inmates excluded from participation under this section are notified of the specific reason(s) by a written explanation of the decision, unless possessing such written information would threaten the safety of the inmate or other legitimate penological interest(s). If prohibited from possessing a copy of the written explanation, inmates remain entitled under the Freedom of Information Act (FOIA) to access this information from their central files, and must be provided reasonable opportunities to access and review such documents. At the inmate's request, expense, and preparation of an envelope, staff may photocopy and mail the documents.

An inmate's exclusion from participation must be based on their individual history of behavior that could jeopardize the legitimate penological interests listed above. Inmates must not be excluded from participation based on general categorizations of previous conduct.

(1) **Sex Offenders.** Inmates whose offense, conduct, or other personal history indicates a propensity to offend through the use of email or jeopardizes the safety, security, orderly operation of the correctional facility, or the protection of the public or staff, should be seriously considered for restriction.

As a method of identifying these inmates, staff responsible for local sex offender management should review inmates with SENTRY CMA Walsh Assignments of Certified, With Conviction, and No Conviction, to determine if their participation in the Public Messaging Service poses a realistic threat. TRULINCS automatically applies a temporary restriction on inmates' accounts with the above SENTRY CMA Walsh Assignments. These restrictions may be over-written when deemed appropriate by staff responsible for local sex offender management and approved by the Warden.

Inmates may be permanently restricted from corresponding and/or communicating with individuals who are:

- Prior child or adult victims of sexual offenses committed by the inmate.
- Children who are being groomed by the inmate for sexual assault or other predatory behavior involving children and/or the caregivers of those children.
- Other sexual offenders.
- Any other contact with the general public deemed inappropriate by staff responsible for local sex offender management due to its association with the inmate's risk to engage in sexually offensive behavior.

(2) **Secure Units.** The Warden may determine which services shall be available to inmates housed in areas of the institution in which there are special security concerns that limit regular access. Special consideration should be given to the type of services being made available in these areas. No services with text input/retention fields (e.g., Contact List Service) shall be available as inmates may use the system to communicate indirectly with other inmates.

At a minimum, workstations located in secure units shall provide access to the following services:

(a) Law Library – per the Program Statement **Inmate Legal Activities**, the Warden shall provide an inmate confined in disciplinary segregation or administrative detention a means to access legal materials.

(b) Purchase TRU-Units – to facilitate charging for printing of law library content, when applicable.

(c) Print – to facilitate printing of law library content, when applicable.

(d) Request to Staff – for reporting of allegations of sexual abuse and harassment directly to the Office of Inspector General (OIG). The Request to Staff Service will not be made available to inmates located in Protective Custody Units (PCU).

Inmates housed in secure units will request access to the TRULINCS workstation per local procedures.

Inmates confined in segregation and PCUs will not have access to the Public Messaging Service. Inmates may continue to receive incoming emails while in secure units that restrict access to the

Public Messaging Service. Staff are not responsible for printing emails for inmates without access to the Public Messaging Service.

b. **Restrictions**

(1) **Inmate Discipline/Criminal Prosecution.** Inmate use of the program in violation of the

procedures subjects the inmate to disciplinary action or criminal prosecution. In addition, inmates who abuse, circumvent, or tamper with the program (equipment, application, furniture) are subject to disciplinary action or criminal prosecution. The DHO or UDC may impose the sanction of loss of Public Messaging or Music/Media Program privileges for inmates found guilty of committing prohibited acts.

Note: Inmates are only restricted from accessing the Music Service during the designated period of time. There is no effect on the MP3 player; therefore, it will continue to operate until it expires.

(2) **Pending Investigation or Disciplinary Action for TRULINCS Abuse or Misuse.** If an inmate is pending either investigation or disciplinary action for possible abuse or misuse, a partial or total restriction is authorized by the Warden. A restriction in this situation is discretionary to ensure the institution's safety, security, and orderly operation, or the protection of the public and staff. When deemed necessary, ordinarily the SIS office recommends this type of restriction. Any TRULINCS restriction recommended by the SIS office may only be imposed with the Warden's approval, in accordance with the procedures outlined in this section and documented on form BP-A0740 Request for Inmate Telephone Restriction or TRULINCS Restriction.

Initial Public Messaging restrictions, imposed pending an investigation or pending disciplinary action for possible TRULINCS abuse or misuse, are limited to 30 days. If additional 30-day periods are required to complete either the investigation or disciplinary process, the Warden must re-authorize the restriction in writing on form BP-A0740, Request for Inmate Telephone or TRULINCS Restriction. Trust Fund staff shall obtain the Warden's approval for reinstatement or continued restrictions every 30 days.

14.10 TRULINCS SERVICES

a. **Account Transactions.** Inmates are responsible for tracking their Commissary, TRUFONE, and TRULINCS account balances. Inmates have access to view account information and transactions for free. Inmates have the ability to print transactional information for a fee.

Inmates that have access to the Account Transactions Service are responsible for printing their own account statements. In rare and unusual circumstances when an inmate demonstrates an imminent need for an account statement and the inmate does not have access to TRULINCS, staff may print the statement and charge the inmate the applicable print fee. Staff prepare the statement and deliver it to the inmate in a secure manner within a reasonable timeframe from the date of the request and at a time that does not interfere with the normal operations of the institution.

b. **Bulletin Board.** TRULINCS offers an electronic bulletin board for posting information for viewing by the inmate population. Departments that opt to use this service are responsible for posting their own documents and the documents' content.

All postings must be in PDF format and may not exceed 2 MB in size.

c. **Contact List.** Inmates may only communicate with approved persons on their contact lists for the purpose of postal mail, TRUFONE, Public Messaging, and/or any person to whom they want to send funds.

It is the inmate's responsibility to maintain their own list with accurate contact information, to include legal first name; legal last name; relationship; language; and postal address. Inmates are subject to disciplinary action for lying and/or providing false or fictitious information regarding a contact (e.g., when complete name is not used; when information is altered to hide the identity of the contact; and any/all other attempts to mislead reviewing and monitoring staff as to the true identity and contact information).

Ordinarily, inmates are limited to having 100 active contacts on their contact list.

Staff are not responsible for printing contact lists for inmates in SHU. However, if an imminent need is demonstrated staff may print a TRULINCS phone list for inmates in SHU. Staff prepare the phone list and deliver it to the inmate in a secure manner within a reasonable timeframe from the date of the request and at a time that does not interfere with the normal operations of the institution.

(1) **Postal Mail.** Inmates are limited to entering two postal addresses for each contact on their list.

Ordinarily, inmates are required to place a TRULINCS-generated mailing label on all outgoing postal mail. The Warden may exempt inmates from this requirement if the Warden determines that an inmate has a physical or mental incapacity, or other extraordinary circumstances that prevents the inmate from using the TRULINCS terminal, or the inmate poses special security concerns prohibiting regular access to TRULINCS terminals (e.g., SHU, SMU).

The Warden may exempt inmates housed in SHU or other areas of the institution in which there are special security concerns that limit regular access to TRULINCS.

If an inmate fails to place the TRULINCS-generated label on outgoing postal mail, the mail is returned to the inmate for proper preparation, in the same way outgoing mail is returned for failure to follow other processing requirements (lack of return address, etc.).

Mailing labels are only placed on outgoing postal mail to identify the recipient. Inmates are prohibited from printing return address labels. Inmates who use mailing labels for other than their intended purpose may be subject to disciplinary action for misuse of Government property.

Ordinarily, inmates are limited to marking for print five mailing labels per day. Inmates may be authorized to print labels in excess of the parameter setting when approved by the Warden or designee.

(2) **Telephone Contacts.** Inmates request that telephone numbers be added to their TRUFONE

lists by creating a contact with a telephone number. Telephone number requests are processed to TRUFONE within approximately 15 minutes.

Ordinarily, inmates are limited to having 30 active telephone numbers on their phone list.

(3) **Public Messaging Contacts.** Inmates request to exchange emails with a person in the community by creating a contact with an email address. Ordinarily, inmates are limited to having 30 active messaging contacts on their list.

Inmates may only exchange emails with contacts who have accepted the inmate's request to communicate. Inmates may not exchange emails with any unauthorized contacts including, but not limited to, victims, witnesses, other persons connected with the inmate's criminal history, law enforcement officers, contractors, vendors who make deliveries of physical goods to the institution (e.g., Commissary, Food Service), and/or volunteers.

Note: Inmates may place attorneys, "special mail" recipients, or other legal representatives on their public email contact list, with the acknowledgment that public emails exchanged with such individuals will not be treated as privileged communications and will be subject to monitoring.

(a) **Consent.** If the contact consents to receive emails, that person is activated on the inmate's email contact list.

(b) **Notices.** Upon receiving the system-generated email, the contact is notified that:

- The Federal inmate identified seeks to add the person in the community to their authorized email contact list.
- The person in the community may approve the inmate for email exchanges, refuse or ignore the request for email exchanges, or refuse the current and all future Federal inmate requests for email exchanges.
- By approving, the person in the community consents to have Bureau staff monitor the content of all emails and agrees to comply with program rules and procedures.

At any time a person in the community may choose to not participate in messaging. Each email received from an inmate will provide the contact with guidance to remove him-/herself from the specific inmate's contact list or refuse all Federal inmates' requests for email exchanges. The guidance is provided within CorrLinks. In addition, each email received from an inmate notifies the person that by utilizing CorrLinks to send/receive emails they consent to have Bureau staff

monitor the informational content of all emails exchanged and to comply with all program rules and procedures.

(c) **Blocking of Email Address(es).** TRULINCS provides three types of email address blocks: Bureau-wide, facility-wide, and inmate-specific. Supporting documentation for blocking email addresses are scanned into TRUFACS using the document imaging process.

Ordinarily, written requests from the Warden or Associate Warden for blocking an email address are processed within one working day after receipt by Trust Fund staff. If specified, these blocks are placed on a specific

inmate account; however, if a specific inmate is not identified or where the request specifically states, a block can be placed to prevent any inmate at the facility from emailing a specific address.

Note: Requests for blocking may not be processed by deleting the contact from an inmate account.

- **Bureau-wide Block.** Request for Bureau-wide blocks should be routed to the Central Office Intelligence Branch for approval. If approved, these blocks will be placed by Central Office TRULINCS staff. These requests can be for a specific email address or an entire domain.
- **Facility-wide Block.** Trust Fund staff place blocks by entering an email address on the Facility Blocked Contact Management Screen in TRULINCS. The authorization of blocking of an email address cannot be delegated below the Associate Warden level.
- **Inmate-Specific Blocks.** The contact email address is blocked within the Contact List administration in TRULINCS.
- **Removal of Blocks.** When an email address is blocked at the recipient's request, the System Administrator removes the block by placing the contact's status to Pending Contact Approval when a written request from the contact is received.

(4) **Inmate to Inmate Communication.** An inmate may be permitted to correspond via Public Messaging and postal mail with an inmate confined in any Bureau facility in accordance with the Program Statement **Correspondence**.

Upon receipt of the approved correspondence from Unit team staff, Trust Fund staff are responsible for entering the approval into TRULINCS and scanning the correspondence into TRUFACS using the document imaging process.

d. **Electronic Law Library.** Inmates use dedicated TRULINCS workstations to access the Electronic Law Library (ELL). Additional guidance regarding law library requirements can be found in the Program Statement **Inmate Legal Activities**.

Trust Fund staff are responsible for ensuring the ELL software is accessible. The Bureau of Prisons Librarian through institution Education staff is responsible for ELL content, functionality, and training.

When inmates do not have access to a printer, Trust Fund staff are responsible for printing ELL documents for inmates with funds. Education staff are responsible for printing ELL documents for inmates without funds. Staff prepares the requested ELL documents and delivers them to the inmate in a secure manner within a reasonable timeframe from the date of the request and at a time that does not interfere with the normal operations of the institution.

e. **Manage Funds**

(1) **Send Funds (BP-199).** Inmates wishing to send funds from their Deposit Fund account via a Request for Withdrawal of Inmate's Personal Funds (BP-199) must add the recipient to their contact list. After the contact is approved, inmates enter a BP-199 and print the applicable BP-199 Form free of charge. See Section 10.2 for additional information regarding BP-199s.

(2) **Pre-Release Account.** Inmates are responsible for managing their own pre-release accounts. See Section 8.11 for information regarding inmate pre-release encumbrances.

(3) **TRUGRAM Gift Funds.** A TRUGRAM is an electronic funds transfer service provided by the Bureau of Prisons through MoneyGram that allows Federal inmates to transfer funds and an associated email to an individual in the public, who can receive the funds at one of MoneyGram's locations throughout the United States, Puerto Rico, Virgin Islands, and Guam.

Inmates may only send TRUGRAMs to approved TRULINCS messaging contacts (Receivers) with active CorrLinks accounts. Receivers must be individuals with government-issued identification. Transfers will not be paid out to companies.

Inmates must consent to MoneyGram's Terms and Conditions prior to sending a TRUGRAM. MoneyGram may report suspicious activity to appropriate law enforcement organizations or other government agencies.

f. **Management TRU-Units.** Inmates are responsible for purchasing/transferring TRU-Units and tracking their account balances.

g. **Music Service.** Inmates that have purchased an authorized MP3 player from the Commissary access the Music Service to activate the player; revalidate the player; and purchase non-explicit media. Inmates are required to accept the Music/Media Terms of Use before accessing the service.

Inmates are authorized to have a maximum of one active MP3 player. Players must be connected to TRULINCS and re-validated every 14 days or they will stop working. It is imperative that MP3 players remain connected to TRULINCS while data is being written to them. The Bureau is not responsible for any damage players receive while charging or while connected to TRULINCS computers. Players may not be used at Bureau privatized facilities or contract holdover facilities.

Media are purchased by inmates within the system using TRU-Units and are priced in three tiers. Many titles/songs have multiple versions and/or multiple artists. Inmates are responsible for ensuring the accuracy of their purchases. All music sales are final; no refunds will be issued. All purchased music/media files must be stored on the MP3 player. Inmates may print a list of their media for a fee.

The music library is automatically updated when made available to the contractor; the Bureau does not control when songs are made available or the library content. However, songs that jeopardize the safety, security, or good order of the institution or protection of the public will be removed from the music library and MP3 players at the Bureau of Prisons' discretion. TRU-Unit refunds will be issued for songs that are removed by the Bureau of Prisons.

The Trust Fund Supervisor shall run the TRULINCS Security Event Report weekly and notify the appropriate staff of potential contraband identified as unauthorized storage devices.

h. **Prescription Refills.** Through an interface with the Bureau Electronic Medical Record (BEMR), inmates are provided with a list of their prescriptions that are eligible to be refilled. Inmates follow established local procedures for picking up requested prescriptions approximately 24 hours after they submit a request.

i. **Print.** Inmates are responsible for printing their own documents and paying print fees when applicable. Inmates are not authorized to possess other inmates' print materials. Inappropriate use of printed materials may result in disciplinary action.

j. **Public Messaging.** The Bureau provides a messaging option for inmates to supplement postal mail correspondence to maintain family and community ties. Both inmates and their contacts must adhere to the rules of this policy, and must not use TRULINCS for any purpose that would jeopardize the safety, security, or orderly operation of the correctional facility, or jeopardize the protection of the public and staff.

(1) **Email Controls.** The maximum number of consecutive minutes an inmate may use the Public Messaging Service is 60 minutes; the interval between sessions is 15 minutes. The Warden may adjust time parameters to ensure the secure and orderly running of the institution.

Emails may not contain attachments and may not exceed 13,000 characters.

Inmates are able to access incoming, outgoing, draft, deleted, and rejected emails for 180 days. Emails older than 180 days are automatically purged from the system.

(2) **Cost of Messaging.** Inmates are charged a per-minute fee while in the Public Messaging Service. Inmates may print their emails for an additional fee.

(3) **Email Holds.** All incoming/outgoing emails are held for a minimum of one hour. When warranted, emails may be held longer. Staff must approve/reject an email while it is on hold or the email will be sent when the hold expires.

(4) **Monitoring.** Emails sent/received by inmates are stored and are subject to monitoring for content by trained staff. If it is determined locally that workload permits, all staff may be assigned to monitor emails. Inmates identified as required monitoring in SENTRY shall have their emails monitored and reviewed.

(5) **Rejection of Public Emails.** TRULINCS allows inmate emails to be routed to staff for review. If a determination is made to reject the correspondence the staff member managing the email must place the email in a Rejected status.

(a) **Authority to Reject Emails.** The authority to manually reject emails is not delegated below the Associate Warden.

(b) **Reasons for Rejection.** Emails that would jeopardize the safety, security, or orderly operation of the correctional facility or the protection of the public and staff may be rejected for reasons that include, but are not limited to:

- The email is detrimental to the security, good order, or discipline of the institution, or a threat to the public and staff, or it might facilitate criminal activity, including any email that:
  - Depicts, describes, or encourages activities that may lead to the use of physical violence or group disruption.
  - Depicts or describes procedures for the construction or use of weapons, ammunition, bombs, or incendiary devices.
  - Depicts, encourages, or describes methods of escape from Bureau facilities.
  - Encourages, instructs, or may facilitate criminal activity (e.g., introduction of contraband).
  - Constitutes unauthorized direction of an inmate's business (see 28 CFR Part 541, subpart B, regarding Inmate Discipline).
  - Contains threats, extortion, or obscenity.
  - Is written in, or otherwise contains, a code.
  - Constitutes sexually explicit material that, by its nature or content, poses a threat to the safety, security, and orderly operation of Bureau facilities, or protection of the public and staff.
  - Depicts or describes procedures for the manufacture of alcoholic beverages or drugs.
- The email otherwise violates the established parameters of the TRULINCS Program.

(c) **Notification of Rejection.** When an email is rejected, the sender is notified that their email will not be delivered and the reason(s) for the rejection. The intended recipient is not informed of the rejection.

(6) **Responsibility for Misuse of the Public Messaging Service.** If either an inmate or a contact attempts to send emails that are rejected, forward inmate emails to an unauthorized address, or otherwise violate this policy, the Warden may remove the individual from participation in this program. Both parties are notified of the removal by the Warden.

(7) **Law Enforcement Requests for Public Emails.** The Bureau's TRULINCS System of Records, and the Privacy Act of 1974, allows disclosure of TRULINCS transactional data and email content as law enforcement uses, as defined therein. Subpoenas for these are not required,

as compared to recorded telephone conversations.

Written requests from law enforcement for emails must demonstrate a need based on an ongoing investigation. Reviews of such requests should be considered by SIS staff, Wardens/Associate Wardens, along with legal staff. Once approved, Bureau staff are authorized to release both transactional data (e.g., date, time, email address, email recipient and sender, and length of the email) and copies of the emails.

k. **Request to Staff.** Inmates wishing to submit a written request to staff must do so using the electronic Request to Staff Service. A written response, if necessary, will be provided. Inmates are limited to submitting five requests per day. The Request to Staff Service will not be made available to inmates located in Protective Custody Units (PCU).

Inmates may report allegations of sexual abuse and harassment directly to the Office of Inspector General (OIG) via the Request to Staff Service.

The Warden may exempt inmates from this requirement if the Warden determines that an inmate has a physical or mental incapacity, or other extraordinary circumstances that prevents the inmate from using the TRULINCS terminal, or the inmate poses special security concerns prohibiting regular access to TRULINCS terminals (e.g., SHU, SMU). Exempted inmates may submit a request in accordance with the Program Statement **Request to Staff, Inmate**.

l. **Survey.** The Bureau has the ability to conduct electronic inmate surveys. Surveys are managed at the national level in accordance with the Program Statement **Research**. Local Trust Fund staff are required to activate the Survey Service on applicable workstations as needed.

14.11 RECORDS MANAGEMENT

The following documents are required to be scanned into TRUFACS using the document imaging process:

a. **Exclusions.** Written requests from the Warden for program or individual service exclusions.

b. **Suspensions and Restrictions.** Documentation (form BP-A0740, Request for Inmate Telephone or TRULINCS Restriction) from the Disciplinary Hearing Officer (DHO) or Unit Discipline Committee (UDC), regarding Public Messaging or Music Restrictions.

In addition, Trust Fund staff must maintain a 30-day file to track temporary restrictions for pending investigations or disciplinary actions submitted on form BP-A0740, Request for Inmate Telephone Restriction or TRULINCS Restriction.

c. **Public Messaging**

- Written approval from the Warden authorizing a Walsh Assignment override.

- Written requests from the Warden or Associate Warden for blocking an email address.
- Written requests from the Warden or Associate Warden for rejecting public emails.
- Requests from contacts for blocking an email address.
- Requests for unblocking an email address must contain a minimum of the contact's full name, email address, inmate's name, inmate's register number, and the request for removing the email address block.

d. **Inmate to Inmate Communication**. Documentation from Unit Managers approving/rejecting inmate to inmate communication.

14.12 SYSTEM MAINTENANCE

a. **Emergency support.** Support is available 7 days a week, 365 days a year from 7:00 a.m.–9:00 p.m. EST. For emergency support call Trust Fund Branch, TRULINCS staff, at 202-514-2555 during office hours (7:00 a.m.- 3:30 p.m. EST); for after-hours emergency support contact the TRULINCS duty phone.

b. **Non-Emergency Technical Assistance.** For non-emergency support use the trouble ticket system or call Trust Fund Branch TRULINCS staff.

c. **Hardware and Software Updates/Improvements.** The Trust Fund Branch initiates the implementation of improved hardware and software. Institution staff are encouraged to provide input and ideas for improving the system and services.