

[REDACTED]

---

**From:** [REDACTED] (USANYE)  
**Sent:** Thursday, October 19, 2017 12:40 PM  
**To:** USANYE-Criminal Chiefs  
**Cc:** [REDACTED] (USANYE); [REDACTED] (USANYE)  
**Subject:** A few items  
**Attachments:** Disco Letter.docx; 2017-10-17 Letter to FD re BOP Email Policy.pdf

Folks,

A few items and updates, some we discussed yesterday and some we did not:

**BOP Inmate Emails:** Attached is the letter we sent to the Federal Defenders regarding our policy regarding BOP inmate emails, as well as our updated discovery letter, which is available on USATabs today. You will likely start hearing from defense counsel in connection with our requests for lists of defense personnel.

[REDACTED]

Please let us know if you have any questions or concerns with respect to any of the above.

Thanks,

[REDACTED]

[REDACTED]  
Chief, Criminal Division  
U.S. Attorney's Office  
Eastern District of New York  
(718) 254-[REDACTED]



**U.S. Department of Justice**

*United States Attorney  
Eastern District of New York*

---

*271 Cadman Plaza East  
Brooklyn, New York 11201*

October 17, 2017

By E-mail

Deirdre D. von Dornum  
Attorney-in-Charge  
Federal Defenders of New York  
Eastern District of New York  
One Pierrepont Plaza, 16th Floor  
Brooklyn, New York 11201

Re: Bureau of Prisons Email Communications

Dear Ms. von Dornum:

I write to provide an update to our Office's policy regarding the production of emails sent and received by defendants during their periods of incarceration at Bureau of Prisons ("BOP") facilities (collectively, "BOP email communications"). As you know, the Office frequently requests that the BOP produce to the government BOP email communications and has taken the position that BOP email communications, including those between a defendant and his or her attorney, are not privileged communications. Nonetheless, the government understands that the BOP now has the technical capability to filter out of its production of BOP email communications emails to and from a particular email address, and the government now agrees to request that the BOP exclude from most productions communications between a defendant and his or her attorneys and other legal assistants and paralegals on their staff.<sup>1</sup>

To allow us to submit such requests to the BOP, the Office requests that upon your Office's assignment to represent a defendant, your assigned attorney send an email to the assigned government attorney with a list of the full email addresses for the assigned attorneys, legal assistants and paralegals who may email with the defendant. If you

---

<sup>1</sup> The Office may request all BOP email communications, including communications between a defendant and his or her attorney, in some limited circumstances. For example, if the Office has reason to believe the communications with an attorney fall within the crime-fraud exception to the attorney-client privilege, the Office may request those emails.

Deirdre D. von Dornum  
October 17, 2017  
Page 2

subsequently wish to provide an email address for an additional attorney, legal assistant or paralegal or change any of the previously-provided email addresses, the Office further requests that the assigned attorney send a subsequent email with the complete list of email addresses, including email addresses that remain unchanged, in the body of the email.

Please contact me if you have any questions about the Office's new procedures.

Very truly yours,

BRIDGET M. ROHDE  
Acting United States Attorney

By:

Chief, Criminal Division  
(718) 254- [REDACTED]



## EOUSA RIF

## MEMORANDUM

U.S. Department of Justice

*United States Attorney's Office  
Eastern District of Kentucky*

---

TO: ALL EMPLOYEES

FROM: Robert M. Duncan, Jr.  
United States Attorney

DATE: December 21, 2018

RE: Office Policy on Implementation and Use of Filter Teams

---

### I. INTRODUCTION

During the course of a criminal or civil investigation, we may come into possession of information that is protected by a privilege, rule, statute, or the Constitution (hereinafter collectively referred to as "privileged information"). The information could come through a search warrant, subpoena, wiretap, receipt of an unsolicited communication, or from an informant. If the prosecution team is exposed to privileged or otherwise confidential information, members of the prosecution team could be disqualified from further involvement in the prosecution, the court may suppress evidence, and, in the most egregious cases, a court may dismiss the indictment. Such a ruling could result in a bar referral and disciplinary action against the prosecuting AUSAs.

The office policy announced herein establishes the procedures for implementation and use of "filter teams" or "taint teams." A "filter team" is a team of AUSA(s) and/or investigator(s), who are separated from the prosecution team in order to protect the defendant's Constitutional and statutory rights by ensuring that the prosecution team is not exposed to privileged information. By implementing a filter team, the government can demonstrate to a court that it has taken adequate precautions to protect the defendant's rights.

The Professional Responsibility Advisory Office (PRAO) advises:

The courts, of course, are the arbiters of what constitutes an "adequate" privilege filter team. Accordingly, adequacy should be assessed not just in terms of actually preventing privileged information from reaching the prosecution team, but also being able to demonstrate successfully to a court that such screening took place. Best practices may include: (1) providing written instructions to the filter team; (2) keeping potentially

privileged materials sealed and labeled, locked or otherwise securely out of the realm of the prosecution team; (3) coordinating procedures with opposing counsel; and (4) permitting court review of challenged documents prior to handing such documents over to the prosecution team. Pre-approval of filter team procedures by a court also may be helpful in that the court would make a prospective determination regarding the adequacy of proposed procedures.

The policy set forth below adopts PRAO's recommended best practices, with modifications specific to the resources and needs of the USAO-EDKY.

## II. WHEN TO USE A FILTER TEAM

A filter team should be used whenever there is a reasonable possibility that materials to be reviewed may include privileged information.

The most common scenario for encountering privileged information is during the execution of a search warrant targeting individuals or entities that are part of a legitimate business or hold themselves out to be one. Privileged information may also be encountered when searching a target's home where the target is known to be represented by an attorney. Though uncommon, a search warrant for an attorney's office would undoubtedly involve privileged material.<sup>1</sup> Searches of electronic service provider accounts, electronic devices, and the interception of communications through a wiretap or recorded jail call may also uncover privileged materials.

The need for a filter team may also arise when a represented defendant engages in ongoing or new illegal activity. The investigation of the new criminal activity could expose privileged contacts between the defendant and his or her attorney on the indicted case. A filter team could be used to direct an investigation into the new criminal activity without running afoul of professional responsibility rules or Constitutional protections afforded the defendant as a result of the indicted crime or complaint. PRAO refers to this scenario as a "new matter filter team."

There may be times when you do not know or anticipate that lawfully-seized evidence contains potentially-privileged information until you are contacted by a defense attorney or you encounter information that appears to be privileged during your review of evidence. Once you are on notice of a potential privilege issue, you have a responsibility to stop your review to ensure that adequate safeguards are taken to protect the defendant's rights.

---

<sup>1</sup> In order to search an attorney's office or otherwise collect evidence directly from an attorney, the prosecution team should follow the guidelines at Section 9-13.420 of the Justice Manual and all other related policies.

### III. WHAT TO DO IF YOU THINK YOU NEED A FILTER TEAM

All AUSAs are responsible for understanding privilege issues and identifying the potential need for a filter team. If you believe there is a reasonable possibility that you will encounter privileged information:

1. Immediately stop reviewing materials that may include privileged information and similarly direct the investigative team to suspend its review.
2. Contact the Executive Assistant United States Attorney (Executive AUSA) to discuss whether a filter AUSA should be assigned to the matter. If a filter team is necessary, the Executive AUSA will direct you to prepare a memo summarizing relevant information about the investigation and specific instructions for transmittal to the filter team.
3. Talk to your case agent about potential privileges and filter procedures. Ask your case agent to have his agency assign a filter agent. Incorporate any necessary instructions specific to your case in the filter team instructions provided to the Executive AUSA.

It is the responsibility of the AUSA to alert members of the prosecution team, including agents/TFOs, paralegals, legal assistants, or other assigned personnel, of the obligation to stop reviewing and notify the AUSA when potentially privileged material is encountered.

### IV. FILTER AUSA RESPONSIBILITIES

There are specially-designated filter AUSAs in the Eastern District of Kentucky. The Ft. Mitchell and London branch offices, and each Lexington litigating division,<sup>2</sup> shall each have at least one designated filter AUSA. Filter AUSAs will be selected by the supervisor of the litigating division and will serve rotating one-year terms. Filter AUSAs will receive or have received training and guidance in reviewing privileged material and filtering information in different types of cases and investigations. The Executive AUSA will assign a designated filter AUSA to appropriate cases. The filter AUSA will not work within the same branch office or litigating division as the prosecution team for that particular case.<sup>3</sup> The filter AUSA will:

1. Carefully review filter team instructions and protocols with filter agent(s) and delineate tasks.

---

<sup>2</sup> For purposes of this policy, these litigating divisions are the Civil Division, Fraud Division, and Criminal Division.

<sup>3</sup> The filter AUSA and the prosecution team may both work in the Lexington office, provided they are not within the same litigating division.

## EOUSA RIF

2. Provide guidance to filter agent(s) on what privileged materials may exist based on the specific facts of the case set forth in the filter instructions.
3. Contact the Litigation Support Unit (LSU) Coordinator to assign the matter to one of the LSU specialists. The LSU Coordinator will then ensure that the assigned LSU specialist is walled off from other work being conducted by the prosecution team on that particular case, consistent with paragraph 6 below. The filter AUSA will coordinate with the assigned LSU specialist to load the discovery into Eclipse or other electronic document-review platform, as necessary based on the nature of the material at issue.
4. Review potentially-privileged materials and identify and segregate privileged materials, non-privileged materials, and potentially-privileged materials. Filter AUSAs shall err on the side of caution and treat any questionable items as potentially privileged.
5. Create a log to document the review process and disposition. At a minimum, the log should include the Bates number of each record reviewed when available, a brief description of the record (date, to/from, subject matter, etc.), its classification as privileged, non-privileged, or potentially privileged, and the nature of the privilege when applicable (attorney-client, work product, etc.).
6. Under no circumstances shall members of the filter team participate in, or provide other assistance to the prosecution team, or convey any privileged information to the prosecution team. The filter team is barred from having any role with respect to the prosecution of the matter.
7. Other than the status of the review, the filter attorney should not discuss or disclose any findings or information reviewed with the prosecution team or any other USAO employee except to the extent necessary to confer with the Executive AUSA.
8. Once the filter team has completed its review and made the appropriate determinations, the filter team AUSA will forward to counsel for the defendant all items that are not privileged and that the filter AUSA intends to provide to the investigating agents and prosecutors. Counsel for the defendant will be given a reasonable time, given the specific circumstances of the case and the nature of the information, to review these materials for privileged information. If the defense attorney claims that an item is privileged and the filter AUSA does not agree, the item shall be submitted to the court under seal for a final determination.
9. Securely store all privileged information. Coordinate with filter agent and the LSU specialist to ensure that privileged materials are removed from evidence available to the prosecution team.

10. Respond to any motions for protective orders or motions relating to privilege issues by explaining that a filter team has been established and the procedures being followed.
11. If the investigation is covert, follow the steps detailed above, except the filter AUSA will wait to provide defense counsel with material determined to be privileged until the investigation is overt. In the covert investigation scenario, it is extremely important to document the steps taken to protect the privilege.

V. BEST PRACTICES

The following is a non-exclusive list of best practices that should be followed in the normal course, recognizing that no two cases are exactly alike and that the needs of each case may vary.

1. If you are seeking a search warrant that may uncover potentially-privileged material, include information in the affidavit that a filter team has been established and will follow an appropriate protocol to avoid disclosure of privileged information.
2. Provide a factual background of the investigation and information about potential privileges to the filter AUSA. Remember that the filter team is a one-way street. The AUSA assigned to the case can fully brief the filter team on relevant background facts regarding the information, but the filter team cannot communicate anything that may contain privileged materials or information directly or indirectly by advising the prosecution team.
3. Identify and provide (or have the filter agent provide) the potentially privileged material to be reviewed (files, computer records, reports, statements, emails etc.) to the filter AUSA. Maintain proper chain of custody of evidence and DO NOT give the filter AUSA original copies of materials. Original evidence that is determined to be privileged should be appropriately marked and secured by the filter agent.
4. If a target or defendant has counsel, the filter AUSA should consult counsel as to any claims of privilege, specific search terms for computers, the identity of members of the defense team including e-mail addresses and/or phone numbers, and suggested procedures unique to the case unless it would impact the integrity of the investigation.

Post-indictment, unless it would threaten an ongoing investigation, the filter AUSA should provide a copy of the filter team instructions to counsel for the defendant and regularly consult with defendant's counsel as necessary.



## EOUSA RIF

5. In cases that have not been indicted, but involve represented targets, the filter AUSA should consult with the target's attorney if doing so would not impact the integrity of the investigation. In instances when the investigation precludes contact with counsel, any doubts about the propriety of disclosure to the prosecution team should be resolved in favor of the defendant and, if necessary, any potentially privileged material should be submitted to a court for review (for example, as a miscellaneous proceeding).
6. If the prosecution team wishes to obtain recorded calls made by a defendant or target while incarcerated, the assigned AUSA must work with the investigating agents and the facility from which the recorded calls are sought to ensure that the facility (a) is aware of the names and contact information of any defense counsel the defendant or target may have communicated with, and (b) has taken appropriate steps to remove such potentially privileged communications from the material provided to the investigating agent or other member of the prosecution team. If those steps have not been taken, or if any member of the prosecution team becomes aware of a reasonable possibility that the material includes attorney-client communications, the assigned AUSA is responsible for implementing a filter team as set forth above in Section III.

Finally, each case is different and should be assessed based on the factual circumstances of the case, including exigencies related to witness security. The filter AUSAs, First AUSA, Executive AUSA, Criminal Chief, Fraud Division Chief, and managers of the London and Ft. Mitchell branch offices will periodically meet to discuss emerging issues and consider revisions to this guidance. AUSAs should contact the Executive AUSA if they have any questions regarding privilege issues.

## VI. NON-ENFORCEABILITY

This document establishes policy for the United States Attorney's Office for the Eastern District of Kentucky. This policy is not intended to, does not, and may not be relied upon to create any rights, privileges, or benefits, procedural or substantive, that are enforceable at law or in equity by any party in any civil or criminal matter. See United States v. Caceres, 440 U.S. 741 (1979). This policy does not place any limitations on the otherwise lawful prerogatives of the United States Attorney's Office for the Eastern District of Kentucky or the United States Department of Justice.

**b. Prisoner Emails**

BOP inmates will commonly have access to the BOP's Trust Fund Limited Inmate Computer System (TRULINCS) - Electronic Messaging service. Inmates and their correspondents must consent to monitoring of all such emails. This applies to emails with attorneys. We can obtain copies of an inmate's TRULINCS emails on request to the BOP. Although, strictly speaking, any privilege that might otherwise apply to communications between an inmate and his or her attorney has been waived, it has been our general practice to avoid looking at emails between inmates and their attorneys. We have often used a "wall" AUSA to look through a BOP TRULINCS production to cull out attorney emails, but that is quite burdensome. Starting in the spring of 2016, BOP became able to cull out emails based on email address, as long as we specify the email address(es) in our original request. In order to comply with our policy of generally avoiding review of attorney-inmate emails, and to avoid burdening a wall AUSA with email review, you should attempt to identify an inmate's attorney(s) prior to making the request to the BOP and ask BOP to cull those from its production to you. (If you believe there is a strong reason we should be reviewing attorney-inmate emails in a given case, you must discuss with the Criminal Chief.)

EOUSA RIP

**From:** [Beall, Thomas \(USAKS\) 1](#)  
**To:** [USAKS-ALL](#)  
**Subject:** New Procedure  
**Date:** Friday, May 26, 2017 3:28:32 PM  
**Attachments:** [Revised Procedure for Requesting and Using Recorded Inmate Phone Calls bo....docx](#)  
[Inmate Phone Calls Request for Authorization \(fillable\).pdf](#)  
[Inmate Phone Calls Request to USMS \(fillable\).pdf](#)

---

Colleagues,

Attached please find a new policy revising and formalizing the procedure for obtaining and handling recordings of inmate telephone calls during investigations involving our office. This policy is the result of collaborative work among AUSA's across the district (and in consultation with EOUSA) with a goal of providing a clear procedure to make appropriate use of this type of evidence and ensure that such cannot be unfairly characterized and criticized. This policy should be implemented immediately with respect to any new requests for recordings. If you have concerns about the application of this policy to any investigations that are currently in process, then please consult with your Criminal Coordinator for specific guidance.

As our cases grow ever more complex, the role this sort of evidence plays in our cases is likely to only increase. Therefore, it is critical that we be able to make use of it in furtherance of our mission, without having the nature of the evidence itself become a distracting and complicating issue. This policy is intended as a tool to do just that – to assist you in making the strongest case possible and ensure that it is not vulnerable to attack.

As always, thank you for all of your hard work, and please enjoy a wonderful and safe holiday weekend with your family and friends,

Tom

Thomas E. Beall  
United States Attorney  
District of Kansas  
444 SE Quincy, Suite 290  
Topeka, KS 66683  
Direct Line: 785 [REDACTED]  
Mobile: 785 [REDACTED]

UNITED STATES DEPARTMENT OF JUSTICE

United States Attorney  
District of Kansas



THOMAS E. BEALL  
U.S. Attorney – District of Kansas

Revision: May 2017



**PROCEDURE FOR REQUESTING AND USING RECORDED  
INMATE PHONE CALLS, VIDEOS AND EMAILS IN  
CRIMINAL AND CIVIL CASES<sup>1</sup>**

**I. Purpose**

In recognition of the well-established attorney-client privilege, the United States Attorney's Office for the District of Kansas (USAO) hereby establishes policy, procedure, and responsibilities regarding requests for the receipt, handling, and use of recorded inmate phone calls, videos and emails<sup>2</sup> obtained from jails, prisons, and/or detention facilities in criminal or civil cases handled by the United States Attorneys' Office for the District of Kansas (USAO).

Inmate calls, videos or emails used by the USAO in any investigation or case may only be obtained through grand jury subpoenas, trial subpoena, administrative subpoena, or specific form described below. The USAO will no longer handle investigations and/or prosecutions with recorded inmate phone calls, videos or emails obtained from facilities without following this policy.<sup>3</sup>

This policy and approval process is consistent with the Department's December 1, 2014, Memorandum regarding Electronic Surveillance Procedures within the Federal Prison System.

A "filter team" will be utilized to shield the prosecution team from being exposed to material that it should not receive under the rules of professional conduct or other laws. Exposure to such material could result in disqualification of members of the prosecution team or suppression of evidence. The use of a filter team may demonstrate that the investigative/prosecution team was not exposed to information to which it was not entitled.

---

<sup>1</sup> This policy does not confer any rights on any person investigated or prosecuted in any federal investigation in the District of Kansas.

<sup>2</sup> For purposes of this policy, any reference to recorded inmate phone calls will include facility videos (of inmates) and inmate emails.

<sup>3</sup> This policy does not address whether audio or video recordings of inmate calls or meetings with their counsel are privileged or confidential in nature. This is not an opinion on the law of privilege and/or when potentially privileged or confidential materials lose their protection, as those are questions of substantive law not considered or addressed in this policy.

## II. Procedure

### A. Approval to Request Recorded Phone Calls or Videos

Any Assistant United States Attorney<sup>4</sup> (AUSA) and/or law enforcement officer working with an AUSA who seeks, in furtherance of an investigation or case, to obtain recorded inmate phone calls, videos or emails from any facility must first complete an internal form entitled "Request for Authorization to Obtain Recorded Inmate Phone Calls" (referred to as Request"). In criminal cases, the branch Criminal Coordinator and Criminal Chief will review and approve the completed form. In civil cases, the branch Civil Coordinator and the Civil Chief will review and approve the completed form.

If the requested information includes an inmate or calls that are the subject of another known investigation or case, the request must be coordinated with the AUSA(s) and law enforcement officers(s) assigned to the other investigation or case. The USAO will not engage in crossover investigations or submit duplicate requests for information from facilities absent this coordination, so pursuit of an effective and efficient manner for proceeding is accomplished. The AUSAs will communicate the coordinated plan to the involved Criminal or Civil Coordinator(s).

When communicating approval of a Request, the branch Criminal or Civil Coordinator will also identify the assigned Filter AUSA. In criminal cases, the Criminal Chief selects Filter AUSAs after consultation with appropriate Civil and/or Criminal Coordinators. In civil cases, the Civil Chief selects Filter AUSAs after consultation with appropriate Civil and/or Criminal Coordinators.

### B. Request to the Facility or United States Marshal

Upon approval, the prosecution team will complete a subpoena or internal form titled "Request to United States Marshal for Recorded Inmate Phone Calls or Videos" (referred to as "USMS Request"), which shall be provided to the facility or the United States Marshals Service (USMS) Office. A copy of each Request, USMS Request and/or subpoena shall be maintained in the case file and central location to be established and maintained by each branch Criminal or Civil Coordinator.

Due to the relationship that the USMS has with facilities holding pre-trial detainees, a USMS Request may be used (rather than a subpoena) to request recorded inmate phone calls or videos. The USMS Request must be completed by an AUSA and provided to Deputy XXX, the USMS Point of Contact in Wichita/Topeka/Kansas City.

Alternatively, if the USAO uses a grand jury subpoena, trial subpoena, or administrative subpoena to obtain the calls or videos, the subpoena should be directed to the custodian of record for the facility. The subpoena must specify each of the following – the inmate's calls requested, the time period covered and request that all calls involving the telephone numbers of all known attorney(s) for the inmate (including office telephone numbers/extensions and cellular phone numbers) be excluded from production. In addition, the period covered by the subpoena should be limited to what is relevant and does not overlap other investigations or cases.

---

<sup>4</sup> Any reference in this policy to an AUSA applies to a Special Assistant United States Attorney (SAUSA).

**C. Filter Team**

When receiving recorded inmate phone calls, videos or emails from an institution, there is a reasonable possibility that communications between an inmate and his/her attorney may be provided. These circumstances warrant the use of filter teams.

The subpoena or USMS Request shall direct production to the filter AUSA or filter team (the team, in addition to an AUSA, may include a law enforcement officer not assigned to the investigation or case). No one involved in the filter team shall be assigned/designated as involved in the specific case at the time the initial request is approved by the Criminal Coordinator and Criminal Chief in criminal cases, or by the Civil Coordinator and Civil Coordinator. The filter AUSA or filter team shall not participate in the investigation or prosecution or civil case that is the subject of the requested information, except to the extent needed to prosecute issues related to the filter process. Supervisory AUSAs and filter AUSAs must take steps to ensure the filter AUSA does not have any investigations or cases connected in any manner to the investigation or prosecution for which the AUSA serves as the filter AUSA. To protect the integrity of the filter, it may be necessary to assign filter AUSAs who are not in the same branch office or division as the prosecuting AUSA(s). Law enforcement officers assigned to the filter team must also take steps to ensure the filter officer has no investigations or cases connected to the filter investigation or prosecution.

**D. Filter Team Process**

The filter team will review the written instructions provided by the Criminal Chief, Civil Chief, or branch Criminal or Civil Coordinator, which will rely on the information provided by the prosecution team.

The filter team must keep all potentially privileged material in a secure manner. This includes sealed, labelled as “potentially privileged or confidential” material, locked, and/or secured in a location not accessible to the prosecution team.

The filter team must use suitable safeguards and conduct all actions in a manner to rebut the presumption that the potentially privileged or confidential material was shared with the prosecution team before the filtering process concluded.

The entirety of recorded phone calls and the index of such calls provided by the institution must be maintained for subsequent review with defense counsel. The filter team will create a duplicate of the recorded phone calls for their review, which will lead to the elimination of any calls between an inmate and their counsel. The duplication will also include a copy for the inmate’s counsel.

The filter team will use the index of phone numbers that accompanied the recorded phone calls to initially remove any recorded phone calls with known attorneys for the inmate. The filter team will use a log to document this preliminary elimination process. Unless the investigation is of ongoing criminal activity of the inmate, this log and duplicate of all recorded phone calls should be provided to inmate’s counsel with an explanation of the filter process to date. Defense counsel will be given a specified period of time to review the remaining phone calls to assert privilege and communicate such to the filter team, with defense counsel’s own privilege log. If the filter team disputes defense counsel’s privilege claim then the filter team will evaluate the merits of the privilege claim with the First

## EOUSA RIF

Assistant United States Attorney and Criminal Chief to evaluate seeking judicial review, which would be handled by the filter AUSA.

Depending upon whether defense counsel is reviewing the recorded phone calls to assert privilege, the filter team will review all remaining recorded phone calls involving phone numbers not known to be associated with the inmate's counsel, to include contractors known to be associated with inmate's counsel, such as defense investigators and forensic experts, etc. If potentially privileged recordings are identified, the filter team will promptly inform the First Assistant United States Attorney and the Criminal Chief in criminal cases or the Civil Chief in civil cases without revealing any content. The potentially privileged recordings must be segregated from the non-privileged recordings. Unless the filter team is awaiting defense counsel to complete a review of the phone recordings to make any privilege assertion, then non-privileged recordings may be provided to the prosecution team. Before providing any materials to the prosecution team, the filter team should fully document the review process and how the prosecution team was excluded from the entire process, especially if any attorney calls were excluded. Additionally, before the filter team relinquishes any recorded phone calls to the prosecution team, it may be useful for the filter AUSA to be instructed by PRAO for guidance in that process.

If the filter team believes the crime fraud exception applies to any of the recorded phone calls, then it will inform the First Assistant United States Attorney and Criminal Chief without revealing any content. If approved by the First Assistant United States Attorney or Criminal Chief, judicial determination of the application of the crime fraud exception will be sought. Any such litigation will be handled by the filter AUSA, unless the First Assistant United States Attorney, Criminal or Civil Chief, and Civil or Criminal Coordinator determine that it is appropriate for the AUSA assigned to the case to do so.

### **E. Handling Recorded Calls, Videos or Emails Obtained from Facilities**

When an inmate's recorded calls, videos or emails are received from a detention facility the materials will be provided to a filter team immediately for safekeeping and review. The filter team will follow the procedures described in paragraph D, above, before providing any of the evidence to the prosecution team or the civil AUSA assigned to the case.

### **F. Exception and Process for Current Recorded Phone Calls**

On the effective date of this policy, recorded inmate calls, facility videos or emails may already be in the possession of some prosecution teams or civil AUSAs. To the extent possible, these prosecution teams or civil AUSAs shall apply this policy to their investigations/cases. For example, if any calls have not been reviewed, the prosecution team should immediately inform the Criminal Coordinator and Criminal Chief to request the assistance of a filter team.

## EOUSA RIF

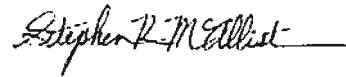
If the prosecution team or civil AUSA has completed the review of any recorded inmate phone calls or videos prior to this policy's effective date, the AUSA should inform the Criminal Coordinator and Criminal Chief, or in civil cases, the Civil Coordinator or Civil Chief, and provide the following:

- Identify defendant(s) charged;
- Case Number (USAO, agency number and court number);
- Case agent and agency;
- Names of inmates whose calls were obtained;
- Time period covered for the phone calls received;
- Process by which the calls were obtained, such as subpoena, USMS request, or other;
- Name of facility that provided the calls;
- Steps taken to ensure there were no attorney inmate phone calls requested or reviewed;
- Whether any calls between an inmate and attorney, were obtained; and
- If any inmate-attorney phone calls were obtained, the steps taken to isolate such calls.



UNITED STATES DEPARTMENT OF JUSTICE

United States Attorney  
District of Kansas



STEPHEN R. MCALLISTER  
U.S. Attorney – District of Kansas

Revision: December 2018



**PROCEDURE FOR REQUESTING AND USING RECORDED  
INMATE PHONE CALLS, VIDEOS AND EMAILS IN  
CRIMINAL AND CIVIL CASES<sup>1</sup>**

---

**I. Purpose**

In recognition of the well-established attorney-client privilege, the United States Attorney's Office for the District of Kansas (USAO) hereby establishes policy, procedure, and responsibilities regarding requests for the receipt, handling, and use of recorded inmate phone calls, videos and emails<sup>2</sup> obtained from jails, prisons, and/or detention facilities in criminal or civil cases handled by the United States Attorneys' Office for the District of Kansas (USAO).

Inmate calls, videos or emails used by the USAO in any investigation or case may only be obtained through grand jury subpoenas, trial subpoena, administrative subpoena, or specific form described below. The USAO will no longer handle investigations and/or prosecutions with recorded inmate phone calls, videos or emails obtained from facilities without following this policy.<sup>3</sup>

This policy and approval process is consistent with the Department's December 1, 2014, Memorandum regarding Electronic Surveillance Procedures within the Federal Prison System.

A "filter team" will be utilized to shield the prosecution team from being exposed to material that it should not receive under the rules of professional conduct or other laws. Exposure to such material could result in disqualification of members of the prosecution team or suppression of evidence. The use of a filter team may demonstrate that the investigative/prosecution team was not exposed to information to which it was not entitled.

---

<sup>1</sup> This policy does not confer any rights on any person investigated or prosecuted in any federal investigation in the District of Kansas.

<sup>2</sup> For purposes of this policy, any reference to recorded inmate phone calls will include facility videos (of inmates) and inmate emails.

<sup>3</sup> This policy does not address whether audio or video recordings of inmate calls or meetings with their counsel are privileged or confidential in nature. This is not an opinion on the law of privilege and/or when potentially privileged or confidential materials lose their protection, as those are questions of substantive law not considered or addressed in this policy.

## EOUSA RIF

### II. Procedure

#### A. Approval to Request Recorded Phone Calls or Videos

Any Assistant United States Attorney<sup>4</sup> (AUSA) and/or law enforcement officer working with an AUSA who seeks, in furtherance of an investigation or case, to obtain recorded inmate phone calls, videos or emails from any facility must first complete an internal form entitled "Request for Authorization to Obtain Recorded Inmate Phone Calls" (referred to as Request"). In criminal cases, the branch Criminal Coordinator and Criminal Chief will review and approve the completed form. In civil cases, the branch Civil Coordinator and the Civil Chief will review and approve the completed form.

If the requested information includes an inmate or calls that are the subject of another known investigation or case, the request must be coordinated with the AUSA(s) and law enforcement officers(s) assigned to the other investigation or case. The USAO will not engage in crossover investigations or submit duplicate requests for information from facilities absent this coordination, so pursuit of an effective and efficient manner for proceeding is accomplished. The AUSAs will communicate the coordinated plan to the involved Criminal or Civil Coordinator(s).

When communicating approval of a Request, the branch Criminal or Civil Coordinator will also identify the assigned Filter AUSA. In criminal cases, the Criminal Chief selects Filter AUSAs after consultation with appropriate Civil and/or Criminal Coordinators. In civil cases, the Civil Chief selects Filter AUSAs after consultation with appropriate Civil and/or Criminal Coordinators.

#### B. Request to the Facility or United States Marshal

Upon approval, the prosecution team will complete a subpoena or internal form titled "Request to United States Marshal for Recorded Inmate Phone Calls or Videos" (referred to as "USMS Request"), which shall be provided to the facility or the United States Marshals Service (USMS) Office. A copy of each Request, USMS Request and/or subpoena shall be maintained in the case file and central location to be established and maintained by each branch Criminal or Civil Coordinator.

Due to the relationship that the USMS has with facilities holding pre-trial detainees, a USMS Request may be used (rather than a subpoena) to request recorded inmate phone calls or videos. The USMS Request must be completed by an AUSA and provided to Deputy XXX, the USMS Point of Contact in Wichita/Topeka/Kansas City.

Alternatively, if the USAO uses a grand jury subpoena, trial subpoena, or administrative subpoena to obtain the calls or videos, the subpoena should be directed to the custodian of record for the facility. The subpoena must specify each of the following – the inmate's calls requested, the time period covered and request that all calls involving the telephone numbers of all known attorney(s) for the inmate (including office telephone numbers/extensions and cellular phone numbers) be excluded from production. In addition, the period covered by the subpoena should be limited to what is relevant and does not overlap other investigations or cases.

---

<sup>4</sup> Any reference in this policy to an AUSA applies to a Special Assistant United States Attorney (SAUSA).

## EOUSA RIF

### C. Filter Team

When receiving recorded inmate phone calls, videos or emails from an institution, there is a reasonable possibility that communications between an inmate and his/her attorney may be provided. These circumstances warrant the use of filter teams.

The subpoena or USMS Request shall direct production to the filter AUSA or filter team (the team, in addition to an AUSA, may include a law enforcement officer not assigned to the investigation or case). No one involved in the filter team shall be assigned/designated as involved in the specific case at the time the initial request is approved by the Criminal Coordinator and Criminal Chief in criminal cases, or by the Civil Coordinator and Civil Coordinator. The filter AUSA or filter team shall not participate in the investigation or prosecution or civil case that is the subject of the requested information, except to the extent needed to prosecute issues related to the filter process. Supervisory AUSAs and filter AUSAs must take steps to ensure the filter AUSA does not have any investigations or cases connected in any manner to the investigation or prosecution for which the AUSA serves as the filter AUSA. To protect the integrity of the filter, it may be necessary to assign filter AUSAs who are not in the same branch office or division as the prosecuting AUSA(s). Law enforcement officers assigned to the filter team must also take steps to ensure the filter officer has no investigations or cases connected to the filter investigation or prosecution.

### D. Filter Team Process

The filter team will review the written instructions provided by the Criminal Chief, Civil Chief, or branch Criminal or Civil Coordinator, which will rely on the information provided by the prosecution team.

The filter team must keep all potentially privileged material in a secure manner. This includes sealed, labelled as “potentially privileged or confidential” material, locked, and/or secured in a location not accessible to the prosecution team.

The filter team must use suitable safeguards and conduct all actions in a manner to rebut the presumption that the potentially privileged or confidential material was shared with the prosecution team before the filtering process concluded.

The entirety of recorded phone calls and the index of such calls provided by the institution must be maintained for subsequent review with defense counsel. The filter team will create a duplicate of the recorded phone calls for their review, which will lead to the elimination of any calls between an inmate and their counsel. The duplication will also include a copy for the inmate’s counsel.

The filter team will use the index of phone numbers that accompanied the recorded phone calls to initially remove any recorded phone calls with known attorneys for the inmate. The filter team will use a log to document this preliminary elimination process. Unless the investigation is of ongoing criminal activity of the inmate, this log and duplicate of all recorded phone calls should be provided to inmate’s counsel with an explanation of the filter process to date. Defense counsel will be given a specified period of time to review the remaining phone calls to assert privilege and communicate such to the filter team, with defense counsel’s own privilege log. If the filter team disputes defense counsel’s privilege claim then the filter team will evaluate the merits of the privilege claim with the First

## EOUSA RIF

Assistant United States Attorney and Criminal Chief to evaluate seeking judicial review, which would be handled by the filter AUSA.

Depending upon whether defense counsel is reviewing the recorded phone calls to assert privilege, the filter team will review all remaining recorded phone calls involving phone numbers not known to be associated with the inmate's counsel, to include contractors known to be associated with inmate's counsel, such as defense investigators and forensic experts, etc. If potentially privileged recordings are identified, the filter team will promptly inform the First Assistant United States Attorney and the Criminal Chief in criminal cases or the Civil Chief in civil cases without revealing any content. The potentially privileged recordings must be segregated from the non-privileged recordings. Unless the filter team is awaiting defense counsel to complete a review of the phone recordings to make any privilege assertion, then non-privileged recordings may be provided to the prosecution team. Before providing any materials to the prosecution team, the filter team should fully document the review process and how the prosecution team was excluded from the entire process, especially if any attorney calls were excluded. Additionally, before the filter team relinquishes any recorded phone calls to the prosecution team, it may be useful for the filter AUSA to be instructed by PRAO for guidance in that process.

If the filter team believes the crime fraud exception applies to any of the recorded phone calls, then it will inform the First Assistant United States Attorney and Criminal Chief without revealing any content. If approved by the First Assistant United States Attorney or Criminal Chief, judicial determination of the application of the crime fraud exception will be sought. Any such litigation will be handled by the filter AUSA, unless the First Assistant United States Attorney, Criminal or Civil Chief, and Civil or Criminal Coordinator determine that it is appropriate for the AUSA assigned to the case to do so.

### E. Handling Recorded Calls, Videos or Emails Obtained from Facilities

When an inmate's recorded calls, videos or emails are received from a detention facility the materials will be provided to a filter team immediately for safekeeping and review. The filter team will follow the procedures described in paragraph D, above, before providing any of the evidence to the prosecution team or the civil AUSA assigned to the case.

### F. Exception and Process for Current Recorded Phone Calls

On the effective date of this policy, recorded inmate calls, facility videos or emails may already be in the possession of some prosecution teams or civil AUSAs. To the extent possible, these prosecution teams or civil AUSAs shall apply this policy to their investigations/cases. For example, if any calls have not been reviewed, the prosecution team should immediately inform the Criminal Coordinator and Criminal Chief to request the assistance of a filter team.

## EOUSA RIF

If the prosecution team or civil AUSA has completed the review of any recorded inmate phone calls or videos prior to this policy's effective date, the AUSA should inform the Criminal Coordinator and Criminal Chief, or in civil cases, the Civil Coordinator or Civil Chief, and provide the following:

- Identify defendant(s) charged;
- Case Number (USAO, agency number and court number);
- Case agent and agency;
- Names of inmates whose calls were obtained;
- Time period covered for the phone calls received;
- Process by which the calls were obtained, such as subpoena, USMS request, or other;
- Name of facility that provided the calls;
- Steps taken to ensure there were no attorney inmate phone calls requested or reviewed;
- Whether any calls between an inmate and attorney, were obtained; and
- If any inmate-attorney phone calls were obtained, the steps taken to isolate such calls.

**Procedure for Requesting and Using Recorded Inmate Phone Calls, Videos and Emails in Criminal and Civil Cases<sup>1</sup>**

I. Purpose

In recognition of the well-established attorney-client privilege, the United States Attorney's Office for the District of Kansas (USAO) hereby establishes policy, procedure, and responsibilities regarding requests for the receipt, handling, and use of recorded inmate phone calls, videos and emails<sup>2</sup> obtained from jails, prisons, and/or detention facilities in criminal or civil cases handled by the United States Attorneys' Office for the District of Kansas (USAO).

Inmate calls, videos or emails used by the USAO in any investigation or case may only be obtained through grand jury subpoenas, trial subpoena, administrative subpoena, or specific form described below. The USAO will no longer handle investigations and/or prosecutions with recorded inmate phone calls, videos or emails obtained from facilities without following this policy.<sup>3</sup>

This policy and approval process is consistent with the Department's December 1, 2014, Memorandum regarding Electronic Surveillance Procedures within the Federal Prison System.

A "filter team" will be utilized to shield the prosecution team from being exposed to material that it should not receive under the rules of professional conduct or other laws. Exposure to such material could result in disqualification of members of the prosecution team or suppression of evidence. The use of a filter team may demonstrate that the investigative/prosecution team was not exposed to information to which it was not entitled.

II. Procedure

A. Approval to Request Recorded Phone Calls or Videos

Any Assistant United States Attorney<sup>4</sup> (AUSA) and/or law enforcement officer working with an AUSA who seeks, in furtherance of an investigation or case, to obtain recorded inmate phone calls, videos or emails from any facility must first complete an internal form entitled "Request for Authorization to Obtain Recorded Inmate Phone Calls"

---

<sup>1</sup> This policy does not confer any rights on any person investigated or prosecuted in any federal investigation in the District of Kansas.

<sup>2</sup> For purposes of this policy, any reference to recorded inmate phone calls will include facility videos (of inmates) and inmate emails.

<sup>3</sup> This policy does not address whether audio or video recordings of inmate calls or meetings with their counsel are privileged or confidential in nature. This is not an opinion on the law of privilege and/or when potentially privileged or confidential materials lose their protection, as those are questions of substantive law not considered or addressed in this policy.

<sup>4</sup> Any reference in this policy to an AUSA applies to a Special Assistant United States Attorney (SAUSA).

(referred to as Request"). In criminal cases, the branch Criminal Coordinator and Criminal Chief will review and approve the completed form. In civil cases, the branch Civil Coordinator and the Civil Chief will review and approve the completed form.

If the requested information includes an inmate or calls that are the subject of another known investigation or case, the request must be coordinated with the AUSA(s) and law enforcement officers(s) assigned to the other investigation or case. The USAO will not engage in crossover investigations or submit duplicate requests for information from facilities absent this coordination, so pursuit of an effective and efficient manner for proceeding is accomplished. The AUSAs will communicate the coordinated plan to the involved Criminal or Civil Coordinator(s).

When communicating approval of a Request, the branch Criminal or Civil Coordinator will also identify the assigned Filter AUSA. In criminal cases, the Criminal Chief selects Filter AUSAs after consultation with appropriate Civil and/or Criminal Coordinators. In civil cases, the Civil Chief selects Filter AUSAs after consultation with appropriate Civil and/or Criminal Coordinators.

**B. Request to the Facility or United States Marshal**

Upon approval, the prosecution team will complete a subpoena or internal form titled "Request to United States Marshal for Recorded Inmate Phone Calls or Videos" (referred to as "USMS Request"), which shall be provided to the facility or the United States Marshals Service (USMS) Office. A copy of each Request, USMS Request and/or subpoena shall be maintained in the case file and central location to be established and maintained by each branch Criminal or Civil Coordinator.

Due to the relationship that the USMS has with facilities holding pre-trial detainees, a USMS Request may be used (rather than a subpoena) to request recorded inmate phone calls or videos. The USMS Request must be completed by an AUSA and provided to Deputy XXX, the USMS Point of Contact in Wichita/Topeka/Kansas City.

Alternatively, if the USAO uses a grand jury subpoena, trial subpoena, or administrative subpoena to obtain the calls or videos, the subpoena should be directed to the custodian of record for the facility. The subpoena must specify each of the following – the inmate's calls requested, the time period covered and request that all calls involving the telephone numbers of all known attorney(s) for the inmate (including office telephone numbers/extensions and cellular phone numbers) be excluded from production. In addition, the period covered by the subpoena should be limited to what is relevant and does not overlap other investigations or cases.

**C. Filter Team**

When receiving recorded inmate phone calls, videos or emails from an institution, there is a reasonable possibility that communications between an inmate and his/her attorney may be provided. These circumstances warrant the use of filter teams.

## EOUSA RIF

The subpoena or USMS Request shall direct production to the filter AUSA or filter team (the team, in addition to an AUSA, may include a law enforcement officer not assigned to the investigation or case). No one involved in the filter team shall be assigned/designated as involved in the specific case at the time the initial request is approved by the Criminal Coordinator and Criminal Chief in criminal cases, or by the Civil Coordinator and Civil Coordinator. The filter AUSA or filter team shall not participate in the investigation or prosecution or civil case that is the subject of the requested information, except to the extent needed to prosecute issues related to the filter process. Supervisory AUSAs and filter AUSAs must take steps to ensure the filter AUSA does not have any investigations or cases connected in any manner to the investigation or prosecution for which the AUSA serves as the filter AUSA. To protect the integrity of the filter, it may be necessary to assign filter AUSAs who are not in the same branch office or division as the prosecuting AUSA(s). Law enforcement officers assigned to the filter team must also take steps to ensure the filter officer has no investigations or cases connected to the filter investigation or prosecution.

### D. Filter Team Process

The filter team will review the written instructions provided by the Criminal Chief, Civil Chief, or branch Criminal or Civil Coordinator, which will rely on the information provided by the prosecution team.

The filter team must keep all potentially privileged material in a secure manner. This includes sealed, labelled as “potentially privileged or confidential” material, locked, and/or secured in a location not accessible to the prosecution team.

The filter team must use suitable safeguards and conduct all actions in a manner to rebut the presumption that the potentially privileged or confidential material was shared with the prosecution team before the filtering process concluded.

The entirety of recorded phone calls and the index of such calls provided by the institution must be maintained for subsequent review with defense counsel. The filter team will create a duplicate of the recorded phone calls for their review, which will lead to the elimination of any calls between an inmate and their counsel. The duplication will also include a copy for the inmate’s counsel.

The filter team will use the index of phone numbers that accompanied the recorded phone calls to initially remove any recorded phone calls with known attorneys for the inmate. The filter team will use a log to document this preliminary elimination process. Unless the investigation is of ongoing criminal activity of the inmate, this log and duplicate of all recorded phone calls should be provided to inmate’s counsel with an explanation of the filter process to date. Defense counsel will be given a specified period of time to review the remaining phone calls to assert privilege and communicate such to the filter team, with defense counsel’s own privilege log. If the filter team disputes defense counsel’s privilege claim then the filter team will evaluate the merits of the privilege claim with the First



## EOUSA RIF

Assistant United States Attorney and Criminal Chief to evaluate seeking judicial review, which would be handled by the filter AUSA.

Depending upon whether defense counsel is reviewing the recorded phone calls to assert privilege, the filter team will review all remaining recorded phone calls involving phone numbers not known to be associated with the inmate's counsel, to include contractors known to be associated with inmate's counsel, such as defense investigators and forensic experts, etc. If potentially privileged recordings are identified, the filter team will promptly inform the First Assistant United States Attorney, and the Criminal Chief in criminal cases or the Civil Chief in civil cases without revealing any content. The potentially privileged recordings must be segregated from the non-privileged recordings. Unless the filter team is awaiting defense counsel to complete a review of the phone recordings to make any privilege assertion, then non-privileged recordings may be provided to the prosecution team. Before providing any materials to the prosecution team, the filter team should fully document the review process and how the prosecution team was excluded from the entire process, especially if any attorney calls were excluded. Additionally, before the filter team relinquishes any recorded phone calls to the prosecution team, it may be useful for the filter AUSA to be instructed by PRAO for guidance in that process.

If the filter team believes the crime fraud exception applies to any of the recorded phone calls, then it will inform the First Assistant United States Attorney and Criminal Chief without revealing any content. If approved by the First Assistant United States Attorney or Criminal Chief, judicial determination of the application of the crime fraud exception will be sought. Any such litigation will be handled by the filter AUSA, unless the First Assistant United States Attorney, Criminal or Civil Chief, and Civil or Criminal Coordinator determine that it is appropriate for the AUSA assigned to the case to do so.

### E. Handling Recorded Calls, Videos or Emails Obtained from Facilities

When an inmate's recorded calls, videos or emails are received from a detention facility the materials will be provided to a filter team immediately for safekeeping and review. The filter team will follow the procedures described in paragraph D, above, before providing any of the evidence to the prosecution team or the civil AUSA assigned to the case.

### F. Exception and Process for Current Recorded Phone Calls

On the effective date of this policy, recorded inmate calls, facility videos or emails may already be in the possession of some prosecution teams or civil AUSAs. To the extent possible, these prosecution teams or civil AUSAs shall apply this policy to their investigations/cases. For example, if any calls have not been reviewed, the prosecution team should immediately inform the Criminal Coordinator and Criminal Chief to request the assistance of a filter team.

## EOUSA RIF

If the prosecution team or civil AUSA has completed the review of any recorded inmate phone calls or videos prior to this policy's effective date, the AUSA should inform the Criminal Coordinator and Criminal Chief, or in civil cases, the Civil Coordinator or Civil Chief, and provide the following:

- Identify defendant(s) charged;
- Case Number (USAO, agency number and court number);
- Case agent and agency;
- Names of inmates whose calls were obtained;
- Time period covered for the phone calls received;
- Process by which the calls were obtained, such as subpoena, USMS request, or other;
- Name of facility that provided the calls;
- Steps taken to ensure there were no attorney inmate phone calls requested or reviewed;
- Whether any calls between an inmate and attorney, were obtained; and
- If any inmate-attorney phone calls were obtained, the steps taken to isolate such calls.

[REDACTED]

**From:** [REDACTED] (USANYS)

EOUSA RIP

**Sent:** Friday, October 06, 2017 10:38 AM

**To:** [REDACTED]@fd.org>

**Cc:** [REDACTED] <[REDACTED]@bop.gov>; Richard Sullivan <Richard\_Sullivan@[REDACTED]>

**Subject:** RE: TRULINCS Email Filter

Thanks [REDACTED]. Just to be clear, my email earlier this morning was not a 'revision,' but more of a response to some of your comments during the call. It is consistent with what I had said in the email previously. As to your first question, we don't have a strong view on how you may want to communicate this to the CJA panel but an email from you with the substance of my emails seems fine. As to your second question re: process, you are correct.

[REDACTED]

**From:** [REDACTED]@fd.org]

**Sent:** Friday, October 06, 2017 8:10 AM

**To:** [REDACTED]@usa.doj.gov>

**Cc:** [REDACTED] <[REDACTED]@bop.gov>; Richard Sullivan <[REDACTED]@nysd.uscourts.gov>

**Subject:** Re: TRULINCS Email Filter

Thank you, [REDACTED]. I appreciate the revision. I think this provides better guidance. Do you mind if I send out the substance of your email to the CJA Panel? Also, to clarify the process, absent an attorney requesting a different address that is acceptable to you, the AUSA will request that BOP screen out the attorney's ECF email address?

On Oct 6, 2017, at 7:23 AM, [REDACTED] (USANYS) <[REDACTED]@usdoj.gov> wrote:

[REDACTED] to follow up, and as you and I discussed yesterday, our Office has now instructed our criminal AUSAs, as a matter of practice, to request that the MCC and MDC filter out attorney-inmate emails in the TRULINCS system for counsel of record when we obtain an inmate's emails, so that those attorney-inmate emails will not be provided to us. There may be very rare exceptions to that general practice – for example, in a crime fraud situation; in acting upon safety concerns or threats; in case of an inmate's disappearance; or where our Office represents the Bureau of Prisons in litigation matters and our AUSAs (either in the Criminal or Civil Division) might need to review all TRULINCS content as part of that representation. Therefore, despite our implementation of this new general practice, we cannot provide you or the defense bar with absolute assurances that attorney-inmate communications sent through the TRULINCS system will never be reviewed. In that regard, the Bureau has been clear that its TRULINCS system is not a vehicle for confidential and privileged communications, and we have been clear that our new practice is not a waiver of

the legal argument that the communications are not privileged. What we have represented to you and have already implemented is a general practice of AUSAs asking the MDC and MCC to filter out communications between inmates and counsel of record, so that our AUSAs will not get or see those in the ordinary course.

**From:** [REDACTED]@fd.org]  
**Sent:** Monday, October 2, 2017 2:53 PM  
**To:** [REDACTED] (USANYS) <[REDACTED]@usa.doi.gov>  
**Cc:** [REDACTED]@bop.gov>; Richard Sullivan  
<Richard\_Sullivan@[REDACTED]>  
**Subject:** RE: TRULINCS Email Filter

Thanks [REDACTED] I'm concerned that the policy set forth below doesn't really solve the problem we set out to solve. If the USAO can review attorney/client emails for any reason whatsoever, we're back at square one. When we all met, my understanding was that you were reserving the right to review attorney/client emails if you believed there was a basis under the crime/fraud exception to privilege. I understand your not wanting to concede that the emails are in fact privileged, but I don't think the guidance below will give attorneys much confidence in the confidentiality of the email system -- which was the point of developing a screening system.

[REDACTED] is the screening system in place?

Thanks,  
[REDACTED]

*Executive Director  
Federal Defenders of New York  
52 Duane Street, 10th Fl.  
New York, NY 10007  
Tel: 212-[REDACTED]  
Fax: 212-511-0392*

<image001.gif> [REDACTED] (USANYS)" --09/27/2017 10:18:13 AM--Gentlemen, this will confirm that, once MCC and MDC give the green light confirming that they are r

**From:** [REDACTED] (USANYS)" <[REDACTED]@usdoj.gov>  
**To:** [REDACTED]@fd.org>, Richard Sullivan <Richard\_Sullivan@[REDACTED]>  
**Cc:** [REDACTED]@bop.gov>  
**Date:** 09/27/2017 10:18 AM  
**Subject:** RE: TRULINCS Email Filter

---

Gentlemen, this will confirm that, once MCC and MDC give the green light confirming that they are ready to implement their TRULINCS screening system, the U.S. Attorney for the Southern District of New York (SDNY) intends to direct our AUSAs to request that MDC and MCC filter out emails between an inmate and his/her attorney-of-record, as a general practice. Please note that SDNY, in adopting this practice, is not taking any position, or waiving any argument it could assert in litigation, that attorney-client emails in the TRULINCS system are not privileged. Further, our general practice of requesting filtering out of such emails

EOUSA RIP

will not necessarily apply when, in our view, circumstances warrant obtaining emails between an inmate and attorney, such as, by way of non-exhaustive example, when we believe a crime fraud is occurring. It is also our understanding that emails sent by an inmate to multiple parties including both attorney and non-attorney contacts will not be filtered out, but rather will be produced to us in the normal course.

EOUSA b6

Chief, Criminal Division  
U.S. Attorney's Office, SDNY  
1 Saint Andrew's Plaza  
New York, NY 10007  
(212) [REDACTED]

From: [REDACTED]@fd.org)  
Sent: Monday, July 10, 2017 9:24 AM  
To: Richard Sullivan <Richard\_Sullivan@[REDACTED]>  
Cc: [REDACTED] (USANYS) <[REDACTED]@usa.doi.gov> [REDACTED]@bop.gov>  
Subject: RE: TRULINCS Email Filter

While it's fresh in my mind, here's a draft of how I will relate the new USAO email procedure when it's ready to go. I'll start with basic background on the issue and explain and attach [REDACTED] letter to Judge Sullivan. And then I'll say this about the USAO:

When it requests a defendant's emails from the TRULINCS system, the U.S. Attorney's Office has agreed to request filtering from the MCC and MDC of the email addresses of all counsel of record as shown on ECF. If you want the USAO to request filtering for a different or additional attorney email address, you must specifically request that from the AUSA on your case. Please note that the USAO has not changed its position that attorney/client emails in the TRULINCS system are not privileged. In addition, the USAO states that it reserves the right to seek attorney/client emails in the TRULINCS system when it believes the crime/fraud exception to the attorney/client privilege applies.

I'd love any thoughts. Thanks,

EOUSA b6

Executive Director  
Federal Defenders of New York  
52 Duane Street, 10th Fl.  
New York, NY 10007  
Tel: 212-512-1000  
Fax: 212-512-0392

Non responsive

Non responsive

Nonresponsive

EOUSA RIP

8:30 is fine for me.

-----Original Message-----

From: Richard\_Sullivan@nysc [mailto:Richard\_Sullivan@nysc]

Sent: Wednesday, July 05, 2017 4:42 PM

To: (USANYS) [mailto:usa.doi.gov]

Cc: EOUSA [mailto:EOUSA@bop.gov]; [mailto:afd.org]

Subject: RE: TROLINCs Email Filter

I hope you all had a great Fourth of July. We're scheduled for a short meeting on the BOP's new email filter on Monday, July 10th at 9:00 am, but I'm wondering if we can start a little earlier -- say 8:30 -- to accommodate a civil trial that I have wrapping up that same day. It turns out that one of the lawyers has an appellate argument in the afternoon, so the parties have requested that we start earlier than usual. Let me know if 8:30 would work; and sorry for the confusion and inconvenience caused by moving things around.

Thanks.

EOUSA b6

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

FROM: /s/  
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

## EOUSA RIF

**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



## EOUSA RIF

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.

## EOUSA RIF

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.

## EOUSA RIF

(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.

## EOUSA RIF

- 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.