DEPARTMENT OF JUSTICE | OFFICE OF THE INSPECTOR GENERAL

MANAGEMENT ADVISORY MEMORANDUM

22-081

MAY 2022

Notification of Concerns with the Absence of a Policy Regarding FBI Employees Emailing Child Sexual Abuse Material and Other Contraband

INVESTIGATIONS DIVISION

May 25, 2022

Management Advisory Memorandum

To: Christopher Wray
Director
Federal Bureau of Investigation

From: Michael E. Horowitz
Inspector General

Subject: Notification of Concerns with the Absence of a Policy Regarding FBI Employees Emailing Child Sexual Abuse Material and Other Contraband

---

The purpose of this memorandum is to advise you of concerns the Department of Justice Office of the Inspector General (OIG) has identified with the absence of a policy regarding the transmission of child sexual abuse material (CSAM) and other contraband material over email by Federal Bureau of Investigation (FBI) employees.[1] The OIG identified these concerns in connection with an investigation of an FBI employee who emailed images the FBI employee believed to contain probable CSAM to a prosecutor with whom the FBI employee was handling a criminal case. While several FBI employees, including the subject of the OIG investigation, told the OIG that CSAM should not be transmitted over email, they could not point us to a written policy that specifically prohibited such conduct. After reviewing a copy of this memorandum, the FBI informed the OIG that it is in the process of deploying new methods to transmit and share CSAM and other sensitive material among law enforcement partners. In this memorandum, the OIG makes one recommendation to address the concerns we identified.

Relevant Authorities

The FBI's Crimes Against Children and Human Trafficking Program Policy Guide, dated August 17, 2021, states the following regarding handling of CSAM:

> CSAM is considered contraband per se and must be handled in accordance with the Digital Evidence Policy Guide…and the Field Evidence Management Policy Guide…. There must be limited access to CSAM, and it must be marked "OBSCENE MATERIAL" on the outside of the envelope containing it, as well as on any external media. As a general rule, CSAM (including any identifying information of a child sexual abuse victim) may not be shared outside the FBI with anyone not having a need to know the information while in the performance of official duties related to the investigation or prosecution in which the child is a victim or a witness

[1] CSAM is the term used by the FBI to refer to child pornography. The FBI has informed the OIG that it believes this term most accurately reflects the sexual abuse and exploitation experienced by child victims.

> (refer to 18 U.S.C. § 3509 for additional information regarding child victims' and child witnesses' rights). CSAM must not be uploaded to Sentinel [the FBI's central recordkeeping system] and must not be stored in the 1A section of an investigative file.

The federal statute that is designed to protect child victims' and child witnesses' rights, 18 U.S.C. § 3509, states, in pertinent part:

> (d) Privacy Protection—
> (1) Confidentiality of Information—
> (A) A person acting in a capacity described in subparagraph (B) in connection with a criminal proceeding shall—
> (i) keep all documents that disclose the name or any other information concerning a child in a secure place to which no person who does not have reason to know their contents has access; and
> (ii) disclose documents described in clause (i) or the information in them that concerns a child only to persons who, by reason of their participation in the proceeding, have reason to know such information.
> (B) Subparagraph (A) applies to—
> (i) all employees of the Government connected with the case, including employees of the Department of Justice, any law enforcement agency involved in the case, and any person hired by the Government to provide assistance in the proceeding....

The FBI's Digital Evidence Policy Guide, dated July 31, 2016, provides that digital evidence generally and contraband specifically must not be uploaded into the FBI's central recordkeeping system (Sentinel) or any other administrative or records management system and identifies FBINET as an example of an administrative or records management system. In addition, the FBI's Field Evidence Management Policy Guide, dated July 23, 2021, provides guidelines on the packaging and storing of CSAM. However, neither the Digital Evidence Policy Guide nor the Field Evidence Management Policy Guide addresses whether CSAM or other digital evidence may be transmitted to other government employees over email.

The FBI also has a policy directive which governs employees' authorized use of the FBI's unclassified network, including its unclassified email system. The directive provides that, except when authorized for official purposes, employees are strictly prohibited from using the FBI unclassified network including the unclassified email system to "access pornographic material," among other things. However, this policy guide does not address how FBI employees should transmit pornographic material or CSAM obtained as evidence in an investigation to other government employees.

The United States Attorneys' Policies and Procedures contain a policy entitled "Safeguarding Child Pornography in the [United States Attorneys' Offices (USAO)]." This policy applies to the Executive Office for United States Attorneys (EOUSA) and all USAOs, and states that child pornography must be:

> Kept under constant physical control by the case [Assistant United States Attorney (AUSA)], his or her designee, or other legally authorized individual involved in the child pornography case.

The United States Attorneys' policy further states:

> Legally authorized employees should use either a virtual desktop environment (VDE) installed on their desktops, or a virtual standalone environment (VSE) installed on a standalone laptop computer to review digitally-stored child pornography within the USAO.

This policy recognizes that there may be circumstances when it is necessary for USAO employees to review child pornography before a VDE or VSE is installed, or circumstances when "networked review" of child pornography is necessary. Regarding those circumstances, the policy provides the following guidelines in a footnote:

> Should review of child pornography be necessary prior to the installation of a VDE and/or a VSE, legally authorized USAO employees should review the materials at a law enforcement facility or using a standalone computer in the USAO. If networked review of the child pornography is necessary, legally authorized employees should contact their system manager in advance to plan for the appropriate sanitization procedures after viewing the child pornography on the network.

The Issue

In connection with an OIG investigation, we discovered that an FBI employee sent images of what the employee believed to be probable CSAM over a secure FBI email system to a prosecutor with whom the FBI employee was handling a criminal case. Several FBI employees told the OIG that CSAM should not be transmitted over email in this manner. In addition, an employee with the Department of Justice Criminal Division's Child Exploitation and Obscenity Section (CEOS) told us that emailing CSAM presents significant risks that the CSAM will be received by unauthorized individuals. An FBI Inspection Division (INSD) employee told us that when it is necessary to transmit images that are believed to be CSAM to other FBI field offices or to the National Center for Missing and Exploited Children, such images should be transmitted through the FBI's closed network system designed for transmitting contraband images.[2]

The FBI informed the OIG that because prosecutors do not have access to the FBI's closed network system unless they request access, agents typically use removable media to provide CSAM images to prosecutors. In addition, after reviewing a draft of this memorandum, the FBI informed the OIG in an official response that, "Common practice and guidance is to provide a standalone computer not connected to an FBI system to review CSAM in a secure space. FBI [e]mployees may also use encrypted removable media to provide CSAM to prosecutors for review on a secure standalone computer." However, the FBI also told us that there is no written FBI policy or directive incorporating this guidance on how FBI employees should transmit CSAM for official purposes. In addition, FBI employees could not point us to an FBI policy that specifically prohibits FBI employees from emailing CSAM or other contraband obtained as evidence in an investigation to prosecutors and other government employees with a need to know the information in their official capacity. While FBI policy prohibits FBI employees from uploading CSAM and other contraband into an administrative or records management system, the FBI informed us that sending contraband over an FBI-administered email system is not considered uploading contraband into an administrative or records management system. The FBI explained that FBINET, which is specifically provided as an example of an administrative or records management system in the FBI's Digital Evidence Policy Guide, is a multifaceted system through which FBI employees have the ability to upload documents in addition to sending email. FBI employees also could not point us to any written policies regarding protecting victim information, such as through encryption, when sending digital evidence, including images of children, over email. Moreover, the United States Attorneys' policy described above does not govern FBI employees.

[2] The National Center for Missing and Exploited Children is a nonprofit organization that has been designated by Congress to receive an annual grant from the Department's Office of Justice Programs, Office of Juvenile Justice and Delinquency Prevention, to operate several programs, including a "child victim identification program to assist law enforcement agencies in identifying victims of child pornography and other sexual crimes to support the recovery of children from sexually exploitative situations." *See* 34 U.S.C. § 11293(b)(1)(K)(ii).

Conclusions

We found that the FBI's written policies do not address the emailing of CSAM and other contraband despite comments we received from the FBI that FBI employees should not do so. We also found that the absence of a written policy presents risks that such contraband will be received by unauthorized individuals. We further believe that the absence of such a policy risks exposing confidential child victim information to unintended recipients, in violation of 18 U.S.C. § 3509.

Recommendations

The OIG recommends the following:

The FBI should clarify its policies regarding the approved methods for transmitting child sexual abuse material (CSAM) and other contraband to prosecutors and other government employees with a need to view the material in their official capacity.

The OIG provided a draft of this memorandum to the FBI, and the FBI's response is incorporated as Appendix 1. The FBI indicated in its response that it agreed with the OIG's recommendation and created a Standard Operating Procedure to address it. Appendix 2 provides the OIG's analysis of the FBI's response and a summary of the action necessary to close the recommendation in this memorandum. The OIG requests that the FBI provide an update on the status of its response to the recommendation within 90 days of the issuance of this memorandum. If you have any questions or would like to discuss the information in this memorandum, please contact me at (202) 514-3435 or Sarah E. Lake, Assistant Inspector General for Investigations, at (202) 616-4730.

cc: Bradley Weinsheimer
Associate Deputy Attorney General
Department of Justice

Appendix 1: The FBI's Response

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

May 24, 2022

The Honorable Michael E. Horowitz
Inspector General
Office of the Inspector General
Department of Justice
950 Pensylvania Ave., N.W.
Washington, DC 20530

Dear Mr. Horowitz:

The Federal Bureau of Investigation appreciates the opportunity to review and respond to your Office's Management Advisory Memorandum *Notification of Concerns regarding the Absence of a Policy Regarding FBI Employees Emailing Child Sexual Abuse Material and Other Contraband.*

We agree that an official program specific policy would ensure child sexual abuse material (CSAM) would only be received by authorized individuals with a need to access the material. Accordingly, we have begun drafting a program specific Standard Operating Procedure (SOP), which will ultimately become part of our Crimes Against Children and Human Trafficking Program Policy Guide.

This new SOP will clearly prohibit the transmission of CSAM via email and delineate the approved methods to transmit CSAM for official purposes. The SOP will include the requirement that FBI employees use encryption software that ensures CSAM being digitally transmitted for official purposes is encrypted at rest and in transit, or require the use of encrypted removable media for use on stand-alone computer systems. Prior to the captioned DOJ MAM, steps by the FBI were already being taken to develop, create and use approved digital transmission platforms comprised of restricted access portals specifically designed for LE-to-LE communications. These platforms are currently being deployed and used in a phased approach across the enterprise.

We appreciate your concern and the courtesy provided to the FBI.

Sincerely,

Luis M. Quesada
Assistant Director
Criminal Investigative Division

Appendix 2: Office of Inspector General Analysis of the FBI's Response

The OIG provided a draft of this memorandum to the FBI, and the FBI's response is incorporated in Appendix 1. The FBI indicated in its response that it agreed with the OIG's recommendation and created a Standard Operating Procedure (SOP) to address it.

The following provides the OIG's analysis of the FBI's response and a summary of the action necessary to close the recommendation. The OIG requests that the FBI provide an update on the status of its response to the recommendation within 90 days of the issuance of this memorandum.

Recommendation: The FBI should clarify its policies regarding the approved methods for transmitting child sexual abuse material (CSAM) and other contraband to prosecutors and other government employees with a need to view the material in their official capacity.

Status: Resolved.

FBI Response: The FBI reported the following:

> We agree that an official program specific policy would ensure child sexual abuse material (CSAM) would only be received by authorized individuals with a need to access the material. Accordingly, we have begun drafting a program specific Standard Operating Procedure (SOP), which will ultimately become part of our Crimes Against Children and Human Trafficking Program Policy Guide.
>
> This new SOP will clearly prohibit the transmission of CSAM via email and delineate the approved methods to transmit CSAM for official purposes. The SOP will include the requirement that FBI employees use encryption software that ensures CSAM being digitally transmitted for official purposes is encrypted at rest and in transit, or require the use of encrypted removable media for use on stand-alone computer systems. Prior to the captioned DOJ MAM, steps by the FBI were already being taken to develop, create and use approved digital transmission platforms comprised of restricted access portals specifically designed for LE-to-LE [law enforcement to law enforcement] communications. These platforms are currently being deployed and used in a phased approach across the enterprise.

OIG Analysis: The FBI's response is responsive to the recommendation. Accordingly, the OIG will consider whether to close this recommendation once the FBI finalizes the new SOP described above and provides a copy of it to the OIG.