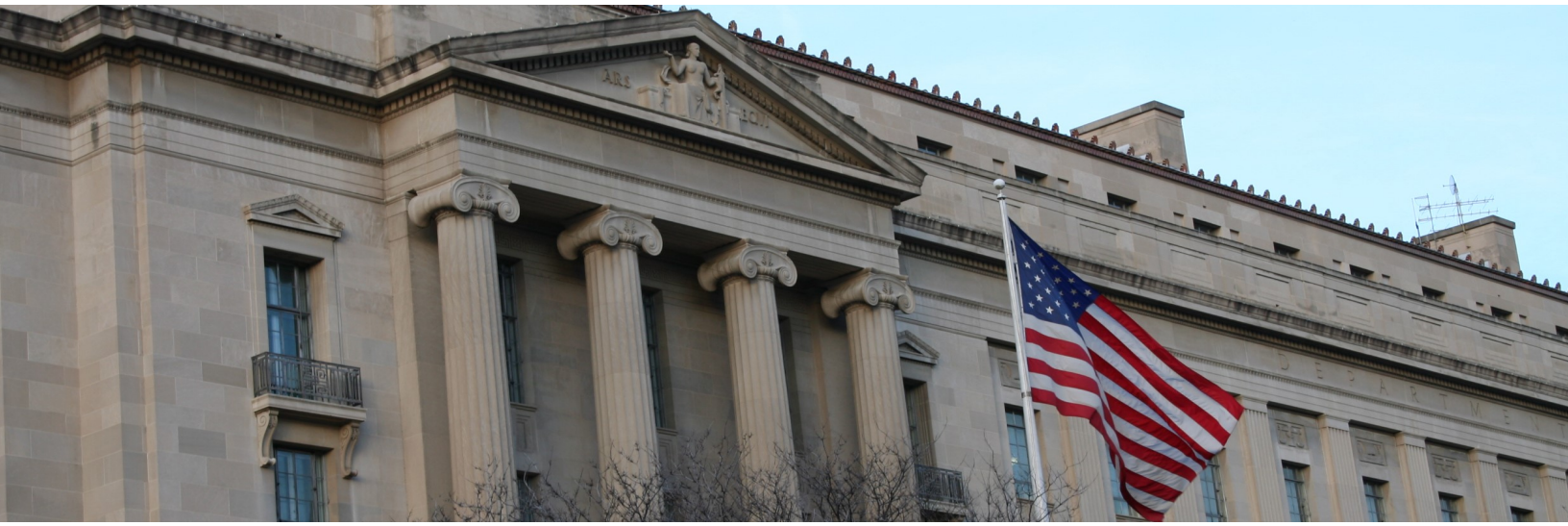
Office of the Inspector General
U.S. Department of Justice

OVERSIGHT ★ INTEGRITY ★ GUIDANCE



Report of Investigation: Recovery of Text Messages From Certain FBI Mobile Devices

REDACTED FOR PUBLIC RELEASE

Redactions were made to the full version of this report to protect individual privacy and information identified by the FBI as law enforcement sensitive.

Investigations Division 2018-003523 December 2018

U.S. Department of Justice
Office of the Inspector General

REPORT OF INVESTIGATION

SUBJECT	CASE NUMBER
UNSPECIFIED	2018-003523

OFFICE CONDUCTINGINVESTIGATION	DOJ COMPONENT
Cyber Investigations Office	Federal Bureau of Investigation

DISTRIBUTION		
☒	Field Office	CYBER
☒	AIGINV	HQ
☒	Component	FBI
☐	USA	
☐	Other	

STATUS

☐ OPEN ☐ OPEN PENDING PROSECUTION ☒ CLOSED

PREVIOUS REPORT SUBMITTED: ☐ YES ☒ NO

Date of Previous Report:

SYNOPSIS

The Department of Justice (DOJ) Office of the Inspector General (OIG) initiated this investigation upon being notified of a gap in text message data collection during the period December 15, 2016, through May 17, 2017, from Federal Bureau of Investigation (FBI) mobile devices assigned to FBI employees Peter Strzok and Lisa Page relevant to a matter being investigated by the OIG's Oversight and Review Division. Specifically, the OIG's Cyber Investigations Office (CYBER) was asked to attempt recovery of these missing text messages for the referenced period from FBI issued mobile devices issued to Strzok and Page.

The OIG asked the FBI Inspection Division to locate the FBI issued Samsung Galaxy S5 devices formerly assigned to the subject employees and to obtain from the same individuals their assigned FBI issued Samsung Galaxy S7 devices. The FBI provided these four devices to the OIG in late January 2018. CYBER utilized digital forensic tools to obtain data extractions from the four FBI issued mobile devices. To ensure the thoroughness of text message recovery efforts, OIG also consulted with the Department of Defense, conducted additional quality assurance steps and hired a Subject Matter Expert. The result of these steps was the recovery of thousands of text messages within the period of the missing text messages, December 15, 2016 through May 17, 2017, as well as hundreds of other text messages outside the gap time period that had not been produced by the FBI due to technical problems with its text message collection tool.

In view of the content of many of the text messages between Strzok and Page, the OIG also asked the Special Counsel's Office (SCO) to provide to the OIG the DOJ issued iPhones that had been assigned to Strzok and Page during their respective assignments to the SCO. Strzok and Page had each returned their

DATE	December 11, 2018	SIGNATURE	[redacted]
PREPARED BY SPECIAL AGENT			
DATE	December 11, 2018	SIGNATURE	Keith A. Bonanno
APPROVED BY SPECIAL AGENT IN CHARGE	Keith A. Bonanno		

DOJ-issued iPhones six months earlier when their assignments to the SCO had ended. The OIG was told that the DOJ issued iPhone previously assigned to Strzok had been re-issued to another FBI agent following Strzok's departure from the SCO. The SCO obtained the iPhone from that individual and provided it to the OIG. CYBER obtained a forensic extraction of the iPhone previously assigned to Strzok; however, this iPhone had been reset to factory settings and was reconfigured for the new user to whom the device was issued. It did not contain data related to Strzok's use of the device. SCO's Records Officer told the OIG that as part of the office's records retention procedure, the officer reviewed Strzok's DOJ issued iPhone after he returned it to the SCO and determined it contained no substantive text messages.

The SCO was unable to locate the iPhone previously assigned to Page, which had been returned to DOJ's Justice Management Division (JMD). Subsequently, in early September 2018, JMD informed the OIG that it had located the iPhone that had been assigned to Page. The OIG took custody of the device. Page's iPhone had been reset to factory settings on July 31, 2017, but had not been reissued to a new user. (The Office of the Deputy Attorney General told the OIG that the Department routinely resets mobile devices to factory settings when the device is returned from a user to enable that device to be issued to another user in the future.) The OIG forensic review of the phone determined that it did not contain any data related to Page's use of the device. SCO's Records Officer stated that she did not receive the phone following Page's departure from the SCO and therefore she did not review Page's iPhone for records that would possibly need to be retained prior to the phone having been reset. As noted on page 395 of the OIG's June 2018 report entitled, "*A Review of Various Actions by the Federal Bureau of Investigation and Department of Justice in Advance of the 2016 Election*," https://www.justice.gov/file/1071991/download, the Department, unlike the FBI, does not have an automated system that seeks to retain text messages, and the service provider only retains such messages for 5 to 7 days.

During calendar year 2017, the FBI phased out use of the Samsung Galaxy S5 devices by its employees and replaced them with Samsung Galaxy S7 devices because of software and other issues that prevented the data collection tool from reliably capturing text messages sent and received via FBI issued Samsung Galaxy S5 mobile devices. According to FBI's Information and Technology Branch, as of November 15, 2018, the data collection tool utilized by FBI was still not reliably collecting text messages from approximately 10 percent of FBI issued mobile devices, which included Samsung S7s and subsequently issued S9s. By comparison, the estimated failure rate of the collection tool was 20 percent for the Samsung S5s.

The OIG reviewed DOJ memoranda and FBI policy relating to retention of substantive electronic communications. These policies require individual employees to take steps to ensure preservation of such electronic communications relating to a criminal or civil investigation. The FBI policy informs its employees to contact the FBI's Enterprise Security Operations Center (ESOC) if they need to access electronic communications that the individual has not preserved, such as text messages and email messages. According to FBI's Office of General Counsel, ESOC has in place a process for the collection of text messages. However, the OIG determined that the FBI does not currently have a specific policy directive mandating that FBI, through ESOC or otherwise, collect text messages sent and received by FBI employees using their FBI issued mobile devices.

Upon reviewing a draft of this report, the FBI requested the opportunity to respond to it. The FBI's response is attached as Appendix 1.

Separate from this report, the OIG will be submitting procedural reform recommendations to the FBI relating to retention of electronic communications.

DETAILS OF THE INVESTIGATION

Predication

The Department of Justice (DOJ) Office of the Inspector General (OIG) initiated this investigation upon being notified of a gap in text message data collection for the period December 15, 2016, through May 17, 2017, from Federal Bureau of Investigation (FBI) mobile devices assigned to FBI employees Peter Strzok and Lisa Page related to a matter being investigated by the OIG's Oversight and Review Division. Specifically, the OIG's Cyber Investigations Office (CYBER) was asked to attempt recovery of the missing text messages for the referenced period from FBI issued mobile devices used by Strzok and Page.

In view of the content of many of the text messages between Strzok and Page, the OIG also asked the Special Counsel's Office (SCO) to provide to the OIG the DOJ issued iPhones that had been assigned to Strzok and Page during their respective assignments to the SCO.

Investigative Process

The OIG's investigative efforts consisted of the following:

Interviews of the following personnel:

- [redacted], Special Counsel's Office (SCO) Executive Officer
- [redacted], SCO Records Officer
- [redacted], SCO Administrative Officer
- [redacted], FBI Supervisory Special Agent
- [redacted], Justice Management Division (JMD) Supervisory Information Technology (IT) Specialist
- [redacted], JMD IT Specialist
- [redacted], JMD IT Specialist
- [redacted], JMD Director
- [redacted], FBI Management Program Analyst
- [redacted], FBI IT Specialist
- [redacted], FBI IT Specialist
- [redacted], FBI IT Specialist
- [redacted], FBI Assistant General Counsel
- [redacted], FBI Unit Chief
- [redacted], FBI Special Assistant

Review of the following:

- DOJ JMD policy documentation regarding electronic messaging record retention
- DOJ Deputy Attorney General Memorandum dated March 30, 2011 regarding Guidance on the Use, Preservation, and Disclosure of Electronic Communications in Federal Criminal Cases
- FBI policy documentation regarding the preservation of electronic communications
- SCO Email for Strzok and Page

Digital Forensic Examination of the following:

- FBI Samsung S5 mobile device previously assigned to Strzok

- FBI Samsung S5 mobile device previously assigned to Page
- FBI Samsung S7 mobile device assigned to Strzok
- FBI Samsung S7 mobile device assigned to Page
- SCO iPhone mobile device previously assigned to Strzok
- SCO iPhone mobile device previously assigned to Page

Additional steps taken to ensure the most complete forensic extraction results:

- Consulted with Department of Defense Computer Forensic Laboratory and utilized a specific tool they recommended
- Conducted additional quality assurance steps regarding a specific database containing repository of text messages
- Hired an Android Subject Matter Expert

Background

On January 12, 2017, the OIG announced the initiation of a review to examine, among other things, "whether the Department and the FBI followed policies or procedures in connection with, or in actions leading up to or related to, the FBI Director's public announcement on July 5, 2016, and the Director's letters to Congress on October 28 and November 6, 2016, and whether certain underlying investigative decisions were based on improper considerations." *A Review of Various Actions by the Federal Bureau of Investigation and Department of Justice in Advance of the 2016 Election*, https://www.justice.gov/file/1071991/download (pre-election review).

As part of the pre-election review, the OIG requested that FBI produce text messages from FBI issued mobile devices assigned to certain FBI employees, including Peter Strzok and Lisa Page. The initial OIG request asked that FBI provide text messages containing specific keywords. Subsequent OIG requests sought all text messages for Strzok and Page for the entire period of the Clinton e-mail server investigation as well as the period of the Russia investigation during which Strzok and Page worked on it. OIG received text message productions from the FBI; however, we noted that no text messages were provided for Page during the period December 15, 2016 to May 17, 2017, and no text messages were provided for Strzok during the period June 18, 2016 through July 5, 2017. Thus, for the period from December 15, 2016, to May 17, 2017, we received no text messages between Page and Strzok, and for the period from June 18, 2016, to December 14, 2016, and from May 18, 2017, to July 5, 2017, the Page-Strzok text messages that we received came solely from Page's text archives.

Strzok was assigned to the FBI's investigation of Hillary Clinton's use of a private email server from August 2015 until July 2016. Page was FBI Deputy Director Andrew McCabe's Special Counsel during the relevant period of the OIG's review and provided support to the investigation from early February 2016 until July 2016. The investigation was resumed by FBI on or about October 28, 2016, and both Strzok and Page were involved in the investigation until it was concluded on or about November 6, 2016. Beginning in July 2016, Strzok was also assigned to investigate allegations of Russian interference in the 2016 Presidential election. Page was involved in that investigation as well based on her position as McCabe's Special Counsel.

On May 17, 2017, the Special Counsel's Office (SCO) was established to investigate alleged Russian interference in the 2016 Presidential election. Strzok and Page were assigned to the SCO shortly thereafter (Strzok in early June; Page on May 28) and were provided DOJ JMD iPhones during their SCO assignment. Based on OIG's examination of their FBI mobile devices, Page and Strzok also retained and continued to use their FBI mobile devices. Specifically, on or about May 18, 2017, Page received an FBI-issued Samsung Galaxy S7 mobile device to replace her previously-issued FBI Samsung Galaxy S5. On or about July 5, 2017,

Strzok received an FBI-issued Samsung Galaxy S7 mobile device to replace his previously-issued FBI Samsung Galaxy S5. Page left the SCO on July 15, 2017. According to SCO, Strzok was removed from the SCO investigation in late July 2017. He completed his Exit Clearance Certification on August 11, 2017 and returned his DOJ issued iPhone on or about that date.

A letter from DOJ Assistant Attorney General Stephen E. Boyd to Chairman Charles E. Grassley, Senate Judiciary Committee, dated January 19, 2018, stated that the FBI's technical system for retaining text messages sent and received on FBI mobile devices failed to preserve text messages for Strzok and Page from December 14, 2016 to approximately May 17, 2017. The letter indicates that the collection tool failure was due to "misconfiguration issues related to rollouts, provisioning, and software upgrades that conflicted with the FBI's collection capabilities."

DOJ Policy and Guidance regarding Electronic Messaging Records Retention

The OIG reviewed DOJ Policy Statement 0801.04, approved September 21, 2016, which establishes DOJ retention policy for email and other types of electronic messaging, to include text messages.

Policy 0801.04 states that electronic messages related to criminal or civil investigations sent or received by DOJ employees engaged in those investigations must be retained in accordance with the retention requirements applicable to the investigation and component specific policies on retention of those messages.

OIG also reviewed DOJ Instruction 0801.04.02, approved November 22, 2016, which provides guidance and best practices on component use of electronic messaging tools and applications for component business purposes.

Section C of 0801.04.02 (Recordkeeping Guidance for Electronic Messaging Tools in Use in the DOJ) subsection 9 (Text Messaging), states that text messaging may be used by staff only if it has been approved by the Head of the Component and in the manner specifically permitted by written component policies. Additional guidance was provided in a memo from the Deputy Attorney General dated March 30, 2011, titled 'Guidance on the Use, Preservation, and Disclosure of Electronic Communications in Federal Criminal Cases.' The memo states that electronic communications should be preserved if they are deemed substantive. Substantive communications include:

- Factual information about investigative activity
- Factual information obtained during interviews or interactions with witnesses (including victims), potential witnesses, experts, informants, or cooperators
- Factual discussions related to the merits of evidence
- Factual information or opinions relating to the credibility or bias of witnesses, informants and potential witnesses; and
- Other factual information that is potentially discoverable under Brady, Giglio, Rule 16 or Rule 26.2 (Jencks Act).

FBI Policy regarding the Collection and Retention of Text Messages

The FBI's Office of General Counsel (OGC) provided FBI Policy Directive 0423D, titled 'Preservation and Disclosure of Electronic Communications in Criminal Cases,' with a last renewal date of October 12, 2016. This policy implements DOJ's Guidance on the Use, Preservation, and Disclosure of Electronic Communications in Federal Criminal Cases as set forth by the Deputy Attorney General on March 30, 2011.

The FBI Policy Directive refers to the preservation of electronic communications in federal criminal cases,

defines what 'substantive' communications are and establishes how these should be preserved by employees. The Directive defines substantive communications as:

15.3. Substantive communication: Factual information about investigative activity; factual information obtained during interviews or interactions with witnesses (including victims), potential witnesses, experts, informants, or cooperators; discussions related to the merits of evidence; and information or opinions relating to the credibility or bias or [sic] witnesses, informants and potential witnesses. Substantive communications may also include agent reports (whether to a colleague, supervisor or prosecutor) about investigative activity, communications that relate to the merits or relative merits of particular evidence, characterizations of potential testimony, interactions with witnesses/victims, and discussions regarding other witness' credibility. Finally, any witness' e-mail, including that of an agent, may constitute impeachment material, Brady material or 3500 material.

Section 8.5.5 of this Policy Directive states that "if employees need to access e-communications that, for whatever reason, have not been preserved, they should address requests to retrieve text messages, PINs, UNet and FBINet e-mails to the Security Division's Enterprise Security Operations Center (ESOC)."

Section 8.6. states, "Employees must not use personal email, personal electronic devices, or social networking sites to communicate about cases or to post case-related or sensitive material. The use of a personal electronic device to send or receive FBI-related e-mail and text messages may subject that personal device and any associated personal e-mail account or personal social networking account to discovery (either directly or via third party subpoena). Apply the 'need to know' principle in determining proper recipients."

Section 11.1.5 states that all employees, "Must not use personal e-mail, personal electronic devices, or social networking sites to communicate about cases or to post case-related or sensitive material."

FBI Assistant General Counsel [redacted] informed OIG that there does not appear to be a directive for preservation of texts by ESOC, but that ESOC retains text messages as a matter of practice. The OIG noted that FBI Policy Directive 0423D informs its employees to contact ESOC if they need to access electronic communications that the individual has not preserved, such as text messages and e-mail messages, thus identifying ESOC as the repository for these types of communications.

FBI ESOC Process for Collection and Retention of Text Messages

ESOC Information Technology Specialists [redacted] and [redacted] informed OIG that FBI uses an automated application to wirelessly collect text messages sent to or from FBI-issued mobile devices. The application collects text message content and other data regarding mobile device usage [redacted]

Although ESOC could not provide a specific explanation for the failure in the FBI's text message collection relating to Strzok's and Page's S5 phones without testing the devices and analyzing the OIG's forensic extractions, [redacted] and [redacted] told the OIG that any one of the following factors could have caused the collection tool failure:

- In calendar year 2016 the collection application vendor reported a "bug" in a version of the collection tool which caused the application to stop collecting text message or log data [redacted]. This application version was replaced by a newer version that corrected the issue in March 2017.
- Errors during the initial installation of the collection application, such as misconfiguration during setup.
- Errors in the collection application's ability to send text message data caused by software updates or operating system updates on the mobile device itself.

- Hardware errors, such as the device not being powered on, being located in a poor cellular signal area, or being located in an area with no cellular service.

According to [redacted] and [redacted], during calendar year 2017, the FBI phased out the Samsung Galaxy S5 devices and replaced them with Samsung Galaxy S7 devices in an effort to correct software and other issues that prevented the data collection tool utilized by ESOC from capturing text messages sent and received via FBI issued Samsung Galaxy S5 mobile devices. Notwithstanding replacement of the Samsung Galaxy S5 devices to address the issue with collection tool failure, according to FBI's Information and Technology Branch, as of November 15, 2018, the data collection tool utilized by FBI was still not reliably collecting text messages from approximately 10 percent of FBI issued mobile devices, which included Samsung S7s and subsequently issued S9s. By comparison, the estimated failure rate of the collection tool was 20 percent with the Samsung S5s..

Weekly reports are generated by FBI's Mobility Program Office (MPO) and shared with FBI Field Offices and Headquarters Division mobile device points of contact to facilitate necessary troubleshooting. According to FBI Inspection Division Unit Chief [redacted] their security team and MPO are actively exploring solutions and proactively working to address the non-compliant devices.

OIG Forensic Analysis of Mobile Devices Utilized by Strzok and Page

Upon OIG's request in late January 2018, FBI provided four FBI issued mobile devices to OIG that had been assigned to Strzok and Page. Strzok and Page each had one Samsung Galaxy S7 that was then-assigned to them and one Galaxy S5 that had been previously assigned to them. OIG's forensic efforts focused on the S5 devices because those were the devices that were in use during the previously identified periods of text message collection tool failure.

OIG digital forensic examiners used forensic tools to recover thousands of text messages from these devices, including many outside the period of collection tool failure (December 15, 2016 to May 17, 2017) and many that Strzok and Page had with persons other than each other. Approximately 9,311 text messages that were sent or received during the period of collection tool failure were recovered from Strzok's S5 phone, of which approximately 8,358 were sent to or received from Page. Approximately 10,760 text messages that were sent or received during the period of collection tool failure were recovered from Page's S5 phone, of which approximately 9,717 were sent to or received from Strzok. Thus, many of the text messages recovered from Strzok's S5 were also recovered from Page's S5. However, some of the Strzok-Page text messages were only recovered from Strzok's phone while others were only recovered from Page's phone. It is important to note that in calculating the number of text messages sent during the period of collection tool failure we only included text messages where the forensic tools recovered the message with an associated date and time. The forensic tools also recovered thousands of other text messages or text message fragments that did not have an associated date or time, and those were not included in calculating these summary numbers.

Additional OIG Forensic Efforts to Recover Text Messages

To further ensure the thoroughness of text message recovery efforts from the two S5 mobile devices, the OIG took several additional steps. First, the OIG consulted with the Department of Defense (DoD), which identified an additional forensic tool that the OIG used to recover additional text messages in the period of collection tool failure, as well as text messages from outside the period of collection tool failure and remnants of additional text messages. Second, the OIG consulted with the FBI's ESOC to determine if it would use any forensic tools in addition to those utilized by OIG to recover text messages from the S5 phones. ESOC did not identify any additional forensic tools. Third, the OIG contracted with a subject matter expert (SME) who specializes in Android device digital forensic examinations to review the physical extraction files acquired by OIG from the two Galaxy S5 devices. The SME was able to recover 62 additional text messages in the period of collection

tool failure, as well as text messages from outside the period of collection tool failure and remnants of additional text messages.

OIG Discovery of Text Messages in Enterprise Database File

During its final quality assurance checks in May 2018, the OIG located an additional cache of text messages in a database identified as "enterprise.db." This was in addition to the OIG's having recovered text messages on the S5 phones in locations where they are typically located through the use of forensic extraction tools. This database appeared to retain a copy of text messages sent and received beginning shortly after the phone was issued until the day the phone was no longer connected to the service provider. The database included text messages sent and received during the period the device was in use, including during the period of the FBI's collection tool failure. Strzok was issued his S5 on or about January 26, 2015 and the enterprise.db had text messages beginning on February 3, 2015. The FBI was unable to determine when Page was issued her S5; however, the database had text messages beginning on February 12, 2016. Additionally, enterprise.db contained other phone activity such as call logs.

Through the extraction of text messages from the enterprise.db database, the OIG recovered 74,385 lines of text messages from Strzok's phone and 52,395 lines of text messages from Page's phone. These text messages included those between Strzok and Page as well as those that they had with other individuals.

In addition, for the period prior to the collection tool failure, when the OIG compared the text messages in the enterprise.db database with those the OIG obtained from FBI ESOC, it became apparent that there were messages found in the enterprise.db database that had not been collected by the FBI's collection program, as well as some messages that were not in the enterprise.db database but that had been collected by the FBI's collection program. As an example, although the FBI's collection program had collected (and therefore produced to the OIG) the text message on August 8, 2016, from Page to Strzok that stated, "He's not ever going to become president, right? Right?!", it had not collected Strzok's response that same day which stated, "No, No he's not. We'll stop it." It was only through the enterprise.db extraction that the OIG obtained this Strzok text message.

The OIG compared the enterprise.db database results with the text message productions from the FBI's collection tool for periods prior to the collection tool failure periods and concluded that the collection tool captured more text messages than enterprise.db; however, there were multiple occasions when text messages found in the enterprise.db database were not collected by the collection tool, even outside the gap period. The missed messages were in groups or single occurrences, some on the same day and some over multiple days. Page's S5 had approximately 44 instances prior to the gap period in which approximately 404 messages were not captured by the collection tool but were captured in enterprise.db, to include the aforementioned exchange on August 8, 2016. One instance involved 57 text messages not collected over the span of several hours.

The OIG noted that there were no discernable patterns regarding the content of text messages missed by the collection tool but captured by enterprise.db, or captured by the collection tool but not found in the enterprise.db database. That is, the OIG found that the content of the text messages did not appear to be a factor in whether they were found in only one of the enterprise.db database or the messages saved by the collection tool; the messages included some political content, some work-related content, and some personal content.

The OIG determined that it was unable to conclude that all text messages were retained because each of the enterprise.db database and the stored messages from FBI's collection tool contained text messages that the other data set did not.

Upon OIG's request, ESOC Information Technology Specialist [redacted] consulted with the FBI's collection

tool vendor, who informed the FBI that the collection application does not write to enterprise.db. [redacted] further stated that ESOC's mobile device team and the vendor believed enterprise.db is intended to track applications with administrative privileges and may have been collecting the logs from the collection tool or another source such as the Short Message Service (SMS) texting application. The collection tool vendor preferred not to share specific details regarding where it saves collected data, maintaining that such information was proprietary; however, [redacted] represented that he could revisit the issue with the vendor if deemed necessary.

OIG digital forensic examiners noted that most Samsung Galaxy S5 devices that they processed, to include non-FBI devices, contained the enterprise.db database. However, the examiners noted that only FBI issued S5 devices contained text message content in the database. OIG consulted with other digital forensic labs, including the Department of Defense experts, who informed the OIG that although they also found the enterprise.db database on Samsung S5 mobile devices that they had examined, they had not found that the database contained text messages.

OIG Contractor Review of Enterprise Database

In addition to retaining the contractor to recover additional text messages as described above, the OIG asked the contractor to review the enterprise.db database and related applications to determine why text messages were being copied to that location on the phones and determine if any of the data was being transmitted to a different location. The contractor's findings included the following:

- Enterprise management software embedded in the Devices from Samsung ("Samsung Knox") was responsible for copying text messages and other data to enterprise.db as a result of device configuration, presumably by a designated mobile device administrator.
- The FBI's collection tool leveraged the Samsung Knox capabilities and had access to data in enterprise.db as well as broad access to the devices. The data stored in enterprise.db was being transmitted from the devices to the collection tool [redacted]. Specifically, data was collected by the tool from enterprise.db via the Samsung Knox capabilities and stored locally by the collection tool application, and then transmitted to the collection tool [redacted].
- The last time the collection tool reported a successful transmission of data for Strzok and Page's S5 devices was June 18, 2016 and December 13, 2016, respectively. This confirms the beginning of the respective collection tool failure period for each device.

Additionally, the contractor informed the OIG that it was unlikely that Strzok and Page attempted to circumvent the FBI's text message collection capabilities, and the OIG found no evidence that they did, as that would require:

- Root access to the devices, which requires a high level of sophistication
- Collection tool or Samsung Knox administrator access, which is unlikely for an employee not tasked with mobile device administration, compliance, monitoring or security.

[redacted]

OIG Contact with Phone Carrier

On January 23, 2018, OIG contacted Verizon Wireless to determine whether the carrier retained text message content. According to Verizon's Legal Department, the content of SMS text messages and/or MMS text

messages is kept three to five days and sometimes up to seven. Their retention period is the same whether the customer is the government or a private citizen. Accordingly, Verizon was not able to produce any text messages for the FBI issued mobile devices in question.

Verizon only has visibility into the text messages sent through their network. They do not have access or visibility into what users store on their phones; therefore, if a user chooses to keep text messages on their phone, Verizon would not be able to access or produce text messages stored on the device outside of their established retention timeframe.

Special Counsel's Office iPhones

The Special Counsel's Office (SCO) Executive Officer informed the OIG that Strzok and Page were part of the initial group of employees assigned to the SCO, Page on May 28, 2017 and Strzok in early June. They were assigned iPhones provided by the Justice Management Division (JMD), Office of the Chief Information Officer (OCIO), Information Technology (IT) staff. Based on the OIG's examination of their FBI mobile devices, Strzok and Page continued to use their FBI devices while assigned to the SCO.

Page left the SCO on July 15, 2017. The SCO Executive Officer completed Page's Exit Clearance Certification, but said that she did not physically receive Page's issued iPhone and laptop. During a phone call, Page indicated to SCO that she had left her assigned cell phone and laptop on a bookshelf at the office on her final day there. The SCO located the laptop but when asked on January 24, 2018, to locate Page's iPhone, the SCO was unable to locate the iPhone. In early September 2018, JMD staff located Page's iPhone and notified OIG, which took custody of the device. Upon examining Page's iPhone, the OIG determined that it had been reset to factory settings on July 31, 2017, but had not been reissued to a new user. The OIG examination found that the iPhone did not contain any data related to Page's use of the device. Neither SCO nor JMD's Office of the Chief Information Officer had records reflecting who handled the device or who reset it after Page turned in her iPhone on July 14, 2017. SCO's Records Officer told the OIG that she did not receive Page's phone following her departure from the SCO and therefore did not review it for records that would possibly need to be retained prior to the phone having been reset. As noted on page 395 of the OIG's June 2018 report entitled, "*A Review of Various Actions by the Federal Bureau of Investigation and Department of Justice in Advance of the 2016 Election*," https://www.justice.gov/file/1071991/download, the Department, unlike the FBI, does not have an automated system that seeks to retain text messages, and the service provider does not retain such messages for more than 5 to 7 days.

According to SCO's Records Officer, Strzok was removed from SCO-related work in late July 2017, and he completed his Exit Clearance Certificate on August 11, 2017. As part of an office records retention procedure, the SCO Records Officer stated that she reviewed Strzok's phone on September 6, 2017. She told the OIG that she determined it did not contain records that needed to be retained. She noted in her records log about Strzok's phone: "No substantive texts, notes or reminders." The SCO Records Officer does not recall whether there were any text messages on Strzok's phone, but said that she made an identical log entry for an iPhone she reviewed from another employee on the same day that she specifically recalled having no text messages. Upon the OIG's request, on or about January 22, 2018, this device was located and provided to the OIG on January 25, 2018. By that time, the device had been re-issued to a new user. OIG conducted forensic analysis of the iPhone and determined that it had been reset to factory settings and reconfigured for the new user to whom it was assigned. It had no content related to Strzok.

Upon reviewing a draft of this report, the Office of the Deputy Attorney General told the OIG that the Department routinely resets mobile devices to factory settings when the device is returned from a user to enable that device to be issued to another user in the future.

OIG's Conclusion

The OIG investigation determined that, although the FBI uses an automated application to wirelessly collect text messages sent to or from FBI-issued mobile devices [redacted] where it is retained by ESOC. Neither the FBI nor the DOJ currently has a policy directive mandating collection and preservation of text messages by ESOC and that the identification and retention of substantive electronic communications is left to the judgment of the individual employee. FBI Policy 0423D guides employees regarding what communications are considered "substantive" and also informs employees that they must not use personal electronic devices to communicate about cases. The OIG noted, however, that FBI policy informs its employees to contact ESOC if they need to access electronic communications that the individual employee has not preserved, such as text messages and email messages, thus identifying ESOC as the repository for these types of communications.

The investigation also determined that the FBI replaced the S5 devices with S7 and S9 devices as part of a regular technical refresh and to address issues with the FBI's text message collection tool. As of November 15, 2018, FBI acknowledged that it continued to experience failure of the collection tool in approximately 10 percent of the mobile devices then in service. The OIG investigation determined that the FBI's collection tool was not only failing to collect any data on certain phones during particular periods of time, it also does not appear that it was collecting all text messages even when it was generally functioning to collect text messages.

The OIG forensically recovered thousands of text messages from FBI mobile devices issued to Strzok and Page through its multiple extraction efforts. Approximately 9,311 text messages were recovered from Strzok's S5 during the collection tool failure period. Approximately 10,760 text messages were recovered from Page's S5 during the collection tool failure period. The OIG's forensic recovery efforts also identified additional relevant text messages from outside the collection tool failure period.

Page resigned from the FBI on May 4, 2018. Strzok's employment was terminated by the FBI on August 10, 2018.

Separate from this report, the OIG will be submitting procedural reform recommendations to the FBI relating to retention of electronic communications.

APPENDIX 1

FBI RESPONSE TO THE REPORT OF THE DEPARTMENT OF JUSTICE'S OFFICE OF THE INSPECTOR GENERAL (Case No. 2018-003523)

The Federal Bureau of Investigation (FBI) welcomes the work of the Department of Justice (DOJ) Office of the Inspector General (OIG) in conducting its investigation and providing its conclusions regarding a gap in the FBI's collection of text messages on mobile devices issued to former FBI employees Mr. Peter Strzok and Ms. Lisa Page. The FBI has been aware of – and acknowledged previously – the fact that although a majority of text messages are captured on its systems, there continue to be challenges in the collection and retention of text messages sent and received on FBI mobile devices. The FBI continues to take steps to mitigate those challenges. While the FBI is refining and improving its collection and retention approach, there are multiple technological, cost, and human factors that must be considered and addressed.

As a general matter, like the DOJ, the FBI meets its legal preservation obligations by implementation of policy and procedural requirements for employees to preserve electronic communications that constitute Federal records or substantive communications, as defined by policy. This preservation obligation applies regardless of the medium of transmission. Beyond these legal obligations, the FBI has a practice of collecting and retaining text messages sent or received on FBI-issued mobile devices. The decision to collect and retain these text messages, including those the FBI is not obligated to preserve, was not imposed by statute, regulation, or Executive Order. The FBI believes that its text collection practices far exceed those of most other Federal agencies.

In the context of capturing and retaining text messages sent or received on FBI-issued devices for business and discovery purposes, despite years of research by the FBI to address the gap issue, and independent research by the DOJ, the FBI is not aware of any solution that closes the collection gap entirely on its current mobile device platforms.[1] Text message collection failure, and rate of collection failure, has been an issue the FBI has worked to understand and correct since its identification in 2014.

Upon recognizing the collection issues and failures, the FBI has performed ongoing research of root causes, potential remediation, and alternatives to the existing collection and retention methods. The FBI believes that no single root cause exists, but rather that several contributing factors, independently or in combination with other factors, may affect collection capability.

The FBI continues to work to improve the collection issue through device upgrades and continues to assess improvements in collection after upgrades occur. The most recent upgrade, to Galaxy S9 devices, is ongoing. The FBI also continues to work to drive down the number of devices not properly reporting or collecting by investigating new or additional software and processes, and by working with vendors, device manufactures, and carriers to develop solutions

[1] It is important to recognize, however, that complete collection of text messages is neither required nor necessary to meet the FBI's legal preservation obligations.

and backstops to device-based collection. Some of these efforts were initiated in early 2016 and are continuing.

Additionally, the FBI is taking parallel actions to address the less technical factors that might affect the rate of collection. These include reorganizing security components to improve communication and coordination, creating appropriate technical teams focused on gap issues, and implementing a device monitoring process to provide alerts and corrective measures when a device is not connecting or reporting properly. Further, in August 2018, the FBI provided additional training to all of its Senior Executive Service personnel, including training on policies and procedures related to the use of FBI-issued mobile devices. Similar mandatory training is being provided to all FBI employees and all employees should have received the training by December 31, 2018.

As to the present OIG report, the gaps in the FBI's general collection of text messages predate the Midyear Exam investigation and the FBI and Special Counsel's Office investigations into Russian influence and interference in the 2016 election. Prior to the OIG's investigation into the FBI's actions in advance of the 2016 election, during at least two unrelated investigations, one of which dates back to 2015, the FBI made the OIG aware of gaps in FBI text message collection capabilities. The FBI accepts the fact that not all texts between Ms. Page and Mr. Strozk were collected by the FBI's text collection tool but appreciates and agrees with the OIG's conclusion and explanation that the content of text messages exchanged between Mr. Strzok and Ms. Page did not appear to be a factor in their collection, or lack thereof. Further, the OIG did not find that the gaps in collection were intentional on the part of the FBI or any FBI personnel.

Regarding the physical devices issued to Ms. Page and Mr. Strzok, in January 2018 the FBI preserved the S5 devices previously assigned to each of them. Those devices, and later the S7 devices issued to Mr. Strzok and Ms. Page, were provided to the OIG upon its request. Because the FBI was acting in a supporting role to the OIG investigation, and in order to avoid even the appearance of a conflict of interest, the FBI did not attempt to exploit any of those devices. As noted by the OIG, because of the level of sophistication and access that would be required, it was unlikely that Ms. Page or Mr. Strzok attempted to circumvent the FBI's text message collection capabilities; and, the OIG found no evidence that they did.

The FBI appreciates this opportunity to provide further background information and context in response to the current report. The FBI is committed to working with the OIG to address its findings and recommendations.

The Department of Justice Office of the Inspector General (DOJ OIG) is a statutorily created independent entity whose mission is to detect and deter waste, fraud, abuse, and misconduct in the Department of Justice, and to promote economy and efficiency in the Department's operations.

To report allegations of waste, fraud, abuse, or misconduct regarding DOJ programs, employees, contractors, grants, or contracts please visit or call the **DOJ OIG Hotline** at oig.justice.gov/hotline or (800) 869-4499.

U.S. DEPARTMENT OF JUSTICE OFFICE OF THE INSPECTOR GENERAL
950 Pennsylvania Avenue, Northwest
Suite 4760
Washington, DC 20530-0001

Website	Twitter	YouTube
oig.justice.gov	@JusticeOIG	JusticeOIG

Also at Oversight.gov