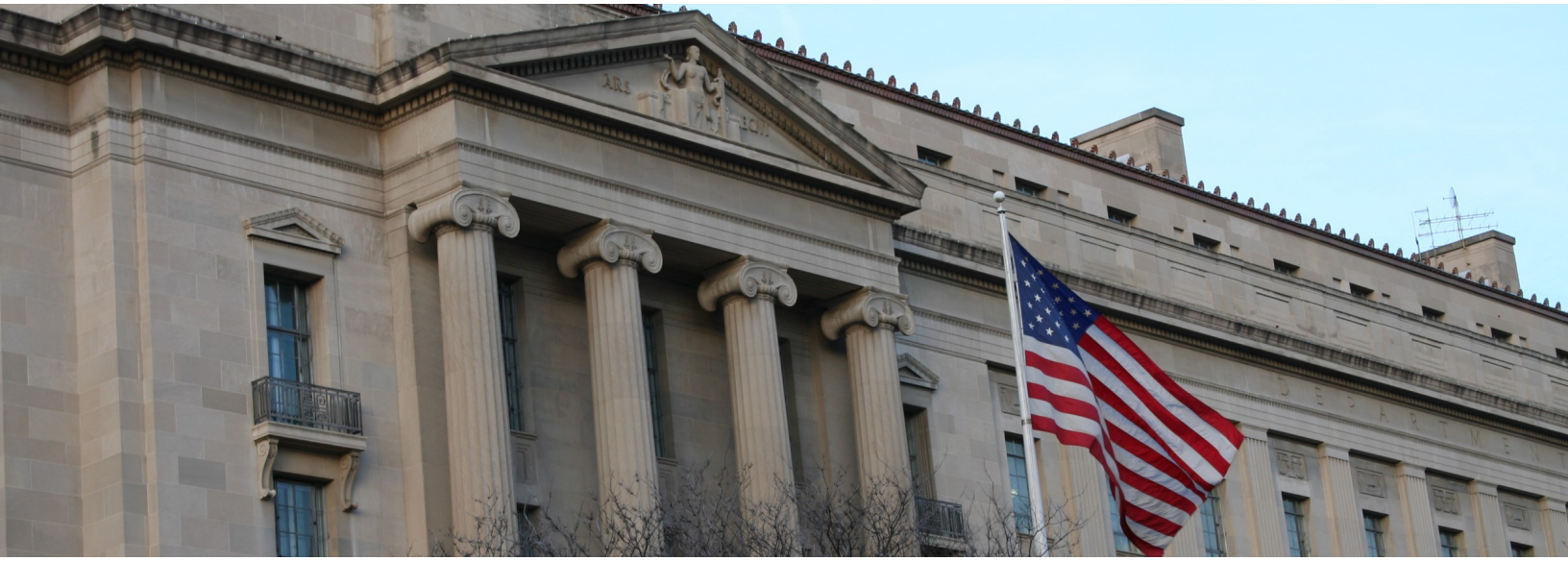
Office of the Inspector General
U.S. Department of Justice

OVERSIGHT ★ INTEGRITY ★ GUIDANCE



Procedural Reform Recommendation for the Federal Bureau of Investigation

Investigations Division

February 2019

PROCEDURAL REFORM RECOMMENDATION FOR THE FEDERAL BUREAU OF INVESTIGATION

SYNOPSIS

The Federal Bureau of Investigation (FBI), Enterprise Security Operations Center (ESOC) uses a commercial, off-the-shelf, automated application to wirelessly collect text messages sent to or from FBI-issued mobile devices. The application is supposed to collect the messages and store them so they are retained by ESOC. ESOC would then have the ability to produce text messages during the discovery process of criminal and civil matters, as well as for internal investigations. During the Office of the Inspector General's (OIG) work that resulted in the report, *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), the OIG found issues with the reliability of the collection application. In addition, unknown to the FBI, the OIG found that FBI text messages were saved to a database on the devices, some of which were not captured by the collection application. The OIG identified this, and other concerns, as security vulnerabilities. The OIG described these issues in its *Report of Investigation: Recovery of Text Messages from Certain FBI Mobile Devices*, https://oig.justice.gov/reports/2018/i-2018-003523.pdf, in which we stated that the OIG would be submitting a procedural reform recommendation to the FBI relating to the retention of electronic communications. We are now doing so.

DETAILS

The Problem

The OIG requested from the FBI text messages of, among others, two employees in connection with the Pre-election Review. When the OIG received the text message production from FBI, there was a time period of several months for which FBI did not produce text messages for mobile devices used by the two FBI employees. The FBI informed the OIG that it was aware that there were deficiencies in its collection application and that it was changing the model of the mobile device issued to FBI employees as part of a regular technical refresh and to mitigate the problem. However, the OIG later learned that, even after upgrading to new devices, the data collection tool utilized by the FBI was still not reliably collecting text messages from approximately 10 percent of more than 31,000 FBI-issued mobile devices.

In addition, during the OIG's forensic examination of FBI mobile devices that were used by the two employees, the OIG discovered a database on the mobile devices containing a plain text repository of a substantial number of text messages sent and received by those devices.

Neither ESOC nor the vendor of the application was aware of the existence, origin, or purpose of this database. OIG analysis of the text messages in the database compared to ESOC productions of text messages during the same time periods when the collection tool was functional identified a significant number of text messages found in the database that were missing from the ESOC production. Furthermore, the Subject Matter Expert with whom the OIG consulted in connection with its forensic analysis of the devices identified additional potential security vulnerabilities regarding the collection application. The OIG has provided these findings to the FBI.

Existing FBI Policy

FBI Policy Directive 0423D, Section 8.5.5 states in part: "if employees need to access e-communications that, for whatever reason, have not been preserved, they should address requests to retrieve text messages . . . to the Security Division's Enterprise Security Operations Center (ESOC)." Although this directive designates ESOC as the repository for text messages, there is no specific policy that requires ESOC to collect and retain text messages.

RECOMMENDATIONS

1. Amend the existing FBI Policy Directive to formally designate an entity to be responsible for text message collection and retention.

2. Conduct additional research and testing of the current collection tool application with the mobile devices deployed by the FBI or seek by other means, in coordination with the collection tool's vendor, to improve reliability of collection and preservation of text messages sent to and from FBI-issued devices, with a goal of 100 percent text message collection and preservation, to the extent technically feasible.

3. Conduct additional research and testing, or seek by other means, prior to procurement of any new collection tool to be used by the FBI to collect and preserve text messages sent to and from FBI-issued devices, with a goal of 100 percent text message collection and preservation, to the extent technically feasible.

4. Coordinate with the collection tool vendor to ensure that data collected by the tool and stored on the device is saved to a secure or encrypted location.

5. Verify and address the security vulnerabilities identified by the Subject Matter Expert with whom the OIG consulted, which have been provided to the FBI. Current and future mobile devices and data collection and preservation tools should be tested for security vulnerabilities in order to ensure the security of the devices and the safekeeping of the sensitive data therein.

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