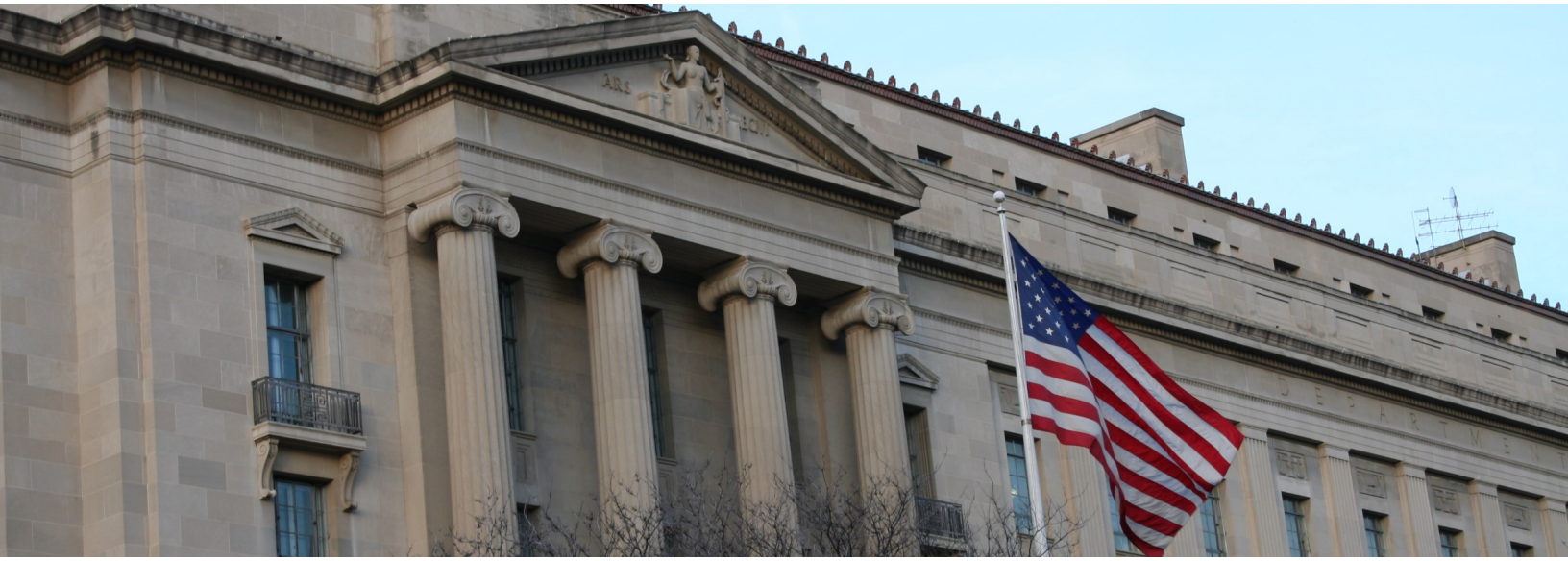
**Office of the Inspector General**
U.S. Department of Justice

**OVERSIGHT ★ INTEGRITY ★ GUIDANCE**



# Management Advisory Memorandum of Concerns Identified with the Federal Bureau of Prisons' Compliance with Department of Justice Requirements on the Use and Monitoring of Computers, Cybersecurity, and Records Retention

Investigations Division 20-028

March 2020

U.S. Department of Justice

Office of the Inspector General

March 2, 2020

MANAGEMENT ADVISORY MEMORANDUM FOR:

MICHAEL CARVAJAL
DIRECTOR
FEDERAL BUREAU OF PRISONS

FROM: MICHAEL E. HOROWITZ
INSPECTOR GENERAL

SUBJECT: Notification of Concerns Identified with the Federal Bureau of Prisons' Compliance with Department of Justice Requirements on the Use and Monitoring of Computers, Cybersecurity, and Records Retention

The purpose of this memorandum is to advise you of concerns raised during two investigations that the Federal Bureau of Prisons (BOP) is not in compliance with several Department of Justice (DOJ) requirements regarding the use and monitoring of computers, cybersecurity, and records retention. Specifically, the Office of the Inspector General (OIG) recently learned that the BOP issues to its employees Samsung mobile devices equipped with a Knox workspace container security solution, which permits users to maintain a so-called "personal container" on the device. In some situations, BOP's failure to educate employees on the appropriate use of the "personal container" on the Samsung devices has led employees who have engaged in inappropriate uses of their mobile devices to claim privacy protections over the content of the "personal container." In this memorandum, the OIG makes four recommendations to address these concerns.

**Relevant Authorities**

Code of Federal Regulations, Title 5, Part 2635.704 states that employees have a duty to protect and conserve Government property and shall not use such property, or allow its use, for other than authorized purposes.

BOP's Standards of Employee Conduct, Section 12, Government Property, also states that government property is to be used for authorized purposes only.

DOJ Order 2740.1A, Use and Monitoring of DOJ Computers and Computer Systems, provides:

> b.(2) While departmental computer systems are provided for official use, some personal use of government computer systems is permitted in accordance with existing policy on personal use of government property, where there is negligible cost to the government and no interference with official business (See 28 C.F.R. § 45.4 [the *de minimis* use policy]).
>
> c. (2)(e) No Expectation of Privacy. Individual employees and contractors should NOT expect privacy in the use of government computers or computer systems. The Department may access e-mail messages, files, records, or other documents on government computer systems whenever it has a legitimate governmental purpose for doing so.

DOJ Order 0904, Cybersecurity Program, provides:

> II.A.12 Planning
> Components must develop, document, update, and implement:
>
> a. Security plans for DOJ information systems that describe the security controls that are in place, or are planned, for the information systems; and
> b. Rules of behavior for individuals who access DOJ information systems.
>
> II. A. 3(b) Awareness and Training
> Components must provide component personnel with training to carry out their assigned information system security-related duties and responsibilities.

DOJ Office of the Chief Information Officer's Mobile Device and Mobile Application Security Supplement 2017 provides:

> Section 2. 2.1, General Plan: All mobile device users shall review and agree to the standard DOJ General Rules of Behavior (ROB) agreement, and any additional Component specific mobile device acceptable use policies, prior to being allowed to use a device to process, transmit, store sensitive DOJ data, or connect to a DOJ network or system.
>
> Section 2, 2.10 (2), Application Management and Restrictions: Container approach- allow users to access commercial apps from commercial app stores. When using the container approach Components shall direct and train users that an App from commercial App stores, to the extent they are unvetted, may pose security risks and may be downloaded only to the Commercial Environment or otherwise isolated from the DOJ data that is

within the Container. This management approach must include the following:

- Creating a Component list of approved, vetted, Apps that may be used within the Container.
- Instituting technical controls that restrict users from installing Apps that are on the DOJ Prohibited Apps list.
  Note: As part of the overall process of App management, Components must establish written Rules of Behavior that address use of mobile Apps. Given the large number of Apps and the wide range of risk that different DOJ Components can tolerate based on mission and other considerations, Component users must agree, in writing, to Component-specific Rules of Behavior for Mobile Devices before receiving a DOJ-owned mobile device. While the Department's general Rules of Behavior provide overall guidance, Components must prepare tailored guidance for areas that the Component CIO determines requires it.

DOJ Guidance on the Use, Preservation, and Disclosure of Electronic Communication in Federal Criminal Cases, dated March 30, 2011, provides guidance regarding employees' use and preservation of electronic communications in light of criminal discovery obligations.

DOJ Justice Manual, 4-1.430-434, outlines DOJ employees' obligations to preserve documents and electronically stored information relevant to civil litigation.

**The Problem**

In connection with the OIG's criminal and administrative investigations, highly relevant evidence is often stored on government-issued electronic devices, and the OIG then needs to extract that evidence from the government-issued devices. During recent OIG investigations involving administrative misconduct by BOP personnel, the OIG learned that the BOP: (a) has not developed, documented, and implemented rules of behavior for employees when accessing and using DOJ electronic systems, as required by DOJ policy; (b) has not required all mobile device users to review and agree to the standard DOJ General Rules of Behavior (ROB) agreement and to any additional BOP-specific rules, as required by DOJ policy; (c) has placed a "personal container" on BOP-issued mobile devices but has not created a list of approved, vetted Apps that may be used within the "personal container," as required by DOJ policy; and (d) has not trained mobile device users on the security risks associated with downloading unvetted Apps onto BOP-issued devices and has

not instituted controls that restrict users from installing Apps on BOP-issued devices that are on the DOJ Prohibited Apps list, as required by DOJ policy.

In the course of a recent OIG investigation, the OIG learned of a BOP employee who misused her BOP-issued Samsung mobile device when the employee (1) used her device to take and send sexually explicit photographs of herself, and (2) intentionally downloaded and used encrypted communication applications, e.g. "chat" applications, on the device to prevent her official communications from being detected by the BOP. The BOP employee told the OIG that she did not think her conduct violated policy regarding the use of the BOP-issued device because the BOP had advised its employees that the mobile devices had a "personal container" for their personal use. The OIG interviewed another BOP employee during this investigation who stated that the BOP did not prohibit or restrict the downloading of encrypted chat applications to BOP-issued devices. The OIG notes that DOJ's Cybersecurity and Privacy Rules of Behavior prohibit installing unauthorized applications or software on DOJ mobile devices.

In the course of a related investigation, the OIG requested that another BOP employee produce her BOP-issued Samsung mobile device to the OIG because the OIG had reason to believe that the device contained evidence that was relevant to its investigation. The BOP employee refused to produce the BOP-issued device, asserting that she was entitled to withhold the device from the OIG because of personal information contained in the "personal container" on the phone. Despite being served with two administrative subpoenas, the BOP employee refused to produce the phone because she believed that she should be able to maintain the privacy of communications and documents transmitted using the "personal container." The OIG successfully petitioned a federal district court to enforce the administrative subpoenas; however, the required litigation impacted our timely access to highly-relevant evidence, delayed our investigation of serious misconduct by a BOP official, and required the OIG to use limited resources to obtain a court order to allow the OIG to access evidence on a government device.

During these investigations, BOP's Chief Information Officer (CIO) told the OIG that BOP has a warning banner that appears when a BOP-issued mobile device is restarted by the employee. However, we also were told that the banner is not displayed on the lock screen of the device.

**Recommendations**

The OIG recommends the following:

1. The BOP should provide component personnel with training to carry out their assigned information system security-related duties and responsibilities, including specific training on how to use BOP-issued

Samsung mobile devices in compliance with these duties and responsibilities.

2. The BOP should refer to the "personal container" on the BOP-issued Samsung mobile phone as the "unsecured container," or "unsecured section" of the phone.

3. The BOP should develop a component-specific ROB agreement that incorporates all the provisions of DOJ's general ROB. The ROB should, among other things,

    a. Make clear that acknowledgement of the ROB agreement indicates consent to monitoring, recording, collection and search of data on all BOP devices, including any "unsecured container," for law enforcement purposes;

    b. Clearly incorporate the *de minimis* use policy;

    c. Address in detail how BOP employees can appropriately use the "unsecured container" on the BOP-issued Samsung mobile device, including specific guidance regarding what applications can be downloaded and how to obtain approval to download such applications.

4. The BOP should incorporate a warning banner that appears on the lock screen of its mobile devices, advising users that activities conducted on the device, including on the "unsecured container," are subject to monitoring and review and that users have no expectation of privacy in any communications conducted on the device.

Please advise us within 60 days of the date of this memorandum on what actions the BOP has taken or intends to take with regard to these issues. If you have any questions or would like to discuss the information in this memorandum, please contact Sarah E. Lake, Assistant Inspector General for Investigations, at (202) 616-4730.

cc: Bradley Weinsheimer
Associate Deputy Attorney General Department of Justice


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, NW
Washington, DC 20530 0001

| **Website** | **Twitter** | **YouTube** |
|---|---|---|
| oig.justice.gov | @JusticeOIG | JusticeOIG |

Also at Oversight.gov