REPORT OF INVESTIGATION

SUBJECT	CASE NUMBER
(b)(6); (b)(7)(C) Assistant United States Attorney (b)(6); (b)(7)(C)	2018-012136

OFFICE CONDUCTING INVESTIGATION	DOJ COMPONENT
Denver Field Office	Executive Office for the United States Attorneys

DISTRIBUTION		STATUS		
☒ Field Office	DNFO	☐ OPEN	☐ OPEN PENDING PROSECUTION	☒ CLOSED
☒ AIGINV		PREVIOUS REPORT SUBMITTED:	☐ YES	☒ NO
☒ Component	EOUSA	Date of Previous Report:		
☐ USA				
☐ Other				

SYNOPSIS

The Department of Justice (DOJ) Office of the Inspector General (OIG) initiated this investigation upon receipt of information from the Executive Office for United States Attorneys (EOUSA) alleging that on (b)(6); (b)(7)(C) (b)(6); (b)(7)(C) Assistant United States Attorney (AUSA) (b)(6); (b)(7)(C) traveled to (b)(6); (b)(7)(C) (b)(6); (b)(7)(C) (b)(6); (b)(7)(C) It was further alleged that (b)(6); (b)(7)(transported and used his DOJ issued smartphone in (b)(6); (b)(7)(C) without proper authorization.

(b)(6); (b)(7)(C)

The OIG investigation (b)(6); (b)(7)(C) (b)(6); (b)(7)(C) did substantiate the allegation that (b)(6); (b)(7)(transported and used his DOJ issued smartphone in (b)(6); (b)(7)(C) without proper authorization. (b)(6); (b)(7)(C) (b)(6); (b)(7)(C)

DATE	April 15, 2022	SIGNATURE	(b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)			
PREPARED BY SPECIAL AGENT			
DATE	April 15, 2022	SIGNATURE	Digitally signed by SANDRA BARNES Date: 2022.04.15 13:28:03 -04'00'
Sandra D. Barnes			
APPROVED BY ACTING SPECIAL AGENT IN CHARGE			

(b)(6); (b)(7)(C)

An OIG review of (b)(6); (b)(7)(C) DOJ issued smartphone billing record for (b)(6); (b)(7)(C) and (b)(6); (b)(7)(C) work emails showed (b)(6); used his DOJ issued smartphone during his (b)(6); (b)(7)(C) personal travel (b)(6); (b)(7)(C) In addition, the review showed that (b)(6); received an email on (b)(6); (b)(7)(C) that was sent to all (b)(6); (b)(7)(C) employees by an (b)(6); (b)(7)(C) security representative stating that all employees were required to obtain prior authorization to take their DOJ issued smartphones on international travel.

In a voluntary interview, (b)(6); admitted he took his DOJ issued smartphone to (b)(6); (b)(7)(C) during his personal trip from (b)(6); (b)(7)(C) without proper authorization. He said he made this decision at the last minute because he needed to stay involved in a high priority (b)(6); (b)(7)(C) case. (b)(6); (b)(7)(said he used "poor judgment" in taking his DOJ issued smartphone to (b)(6); (b)(7)(C) and that he was "pretty sure" there was an office policy regarding the need to obtain prior approval to take a DOJ issued smartphone on international travel.

The DOJ Mobile Device and Mobile Application Security Supplement classifies (b)(6); (b)(7)(C) as a "High Risk Travel Country" and includes special requirements for the use of DOJ issued mobile devices in (b)(6); (b)(7)(C) Among the requirements is the provision that "devices that return from (b)(6); must be fully wiped and re-imaged with the High Risk Profile settings outlined in Appendix D implemented. **These mobile devices will** be placed in a dedicated travel pool and exclusively used for travel to (b)(6); (b)(7)(C) from that point forward." Similarly, (b)(7)(E)

(b)(7)(E)

(b)(7)(E) In August 2018, (b)(6); (b)(7)(C) did not maintain a pool of mobile devices that were used by employees for foreign travel.

(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C) resigned from his position at the United States Attorney's Office (USAO) effective (b)(6); (b)(7)(C)

The OIG has completed its investigation and is providing this report to EOUSA and the Department's Office of Professional Responsibility for appropriate action.

Unless otherwise noted, the OIG applies the preponderance of the evidence standard in determining whether DOJ personnel have committed misconduct. The Merit Systems Protection Board applies this same standard when reviewing a federal agency's decision to take adverse action against an employee based on such misconduct. See 5 U.S.C. § 7701(c)(1)(B); 5 C.F.R. § 1201.56(b)(1)(ii).

ADDITIONAL SUBJECTS

(b)(6); (b)(7)(C)

DETAILS OF INVESTIGATION

Predication

The Department of Justice (DOJ) Office of the Inspector General (OIG) initiated this investigation upon receipt of information from the Executive Office for United States Attorneys (EOUSA) alleging that on (b)(6); (b)(7)(C) (b)(6); (b)(7)(C) Assistant United States Attorney (b)(6); (b)(7)(C) traveled to (b)(6); (b)(7)(C) (b)(6); (b)(7)(C) (b)(6); (b)(7)(C) It was further alleged that (b)(6); (b)(7)(transported and used his DOJ issued cell phone in (b)(6); (b)(7)(C) without proper authorization.

(b)(6); (b)(7)(C)

Investigative Process

The OIG's investigative efforts consisted of the following:

Interviews of the following (b)(6); (b)(7)(C) personnel:

- (b)(6); (b)(7)(C) Assistant United States Attorney
- (b)(6); (b)(7)(C)

Review of the following documents:

- DOJ email account for (b)(6); (b)(7)(C)
- Verizon invoice for the DOJ smartphone assigned to (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C) resigned from his position at the USAO effective (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

Unauthorized Use of DOJ Issued Mobile Device in (b)(6); (b)(7)(C)

The information provided to the OIG alleged that on (b)(6); (b)(7)(C) transported and used his DOJ issued smartphone in (b)(6); (b)(7)(C) during a personal trip without DOJ authorization.

DOJ Order Number 0904: Cybersecurity Program, approved on September 15, 2016, Section II, Subsection D states "[t]he use of DOJ mobile devices (e.g., tablet devices and smartphones) outside the United States must follow the requirements in the DOJ's *Mobile Device and Mobile Application Security Policy Instruction*."

Section F.1.1 of the Department's Mobile Device and Mobile Application Security Supplement 2017 A, dated June 23, 2017, classifies (b)(6); as a High-Risk Travel Country and imposes special requirements for DOJ issued mobile device usage in (b)(6); (b)(7)(C) Under section F.1.1.1 of this security supplement, certain requirements "must be adhered to for all Department of Justice mobile devices being taken on international travel." Those requirements include:

> FT-02: "All Foreign Travel with a DOJ mobile device must be approved prior to allowing the device to leave the US or US territory. . . . For travel to high risk countries Department-level approval must be obtained from the DOJ CISO / OCIO CSS Director prior to travel. . . ."
>
> FT-06: "For High Risk Countries, all DOJ data shall be restricted to Department CISO approved secure container solutions or the device must be running a Department CISO approved advanced monitoring tools at all times. . . ."
>
> FT-11: "All devices must be immediately submitted to the user's Component Security Office, or trained delegate, upon return from foreign travel to be analyzed for potential compromise and/or device

firmware restoration. . . . Based on the cyber risk when traveling to the [sic] (b)(6); (b)(7)(C) the mobile device (i.e., smartphone, tablet) must be returned and removed from use by the Component Security Office upon the user's return. The devices that return from (b)(6); (b)(7)(C) must be fully wiped and re-imaged with the High-Risk Profile settings outlined in Appendix E, 10.1, implemented. These mobile devices will be placed in a dedicated travel pool and exclusively used for travel to (b)(6); (b)(7)(C) from that point forward."

FT-12: "High Risk Countries – Users shall not connect to cellular data or device services in the country. Users shall only use Government furnished mobile W-Fi Hot Spots or MiFi devices, for data connectivity or Government controlled and maintained Wi-Fi access points running a minimum of WPA2. All devices roaming capabilities shall be disabled. . . ."

FT-13: "High Risk Countries – Users shall only connect to DOJ provided mobile wireless hot spots or US Government Control and maintained Wireless Access Points. All Wi-Fi connections must be secured with a minimum of WPA2."

In addition, section F.5 of the security supplement describes in detail the foreign travel request process and reiterates these security requirements.

(b)(7)(E)

In describing the rules for foreign travel using government issued devices, (b)(7)(E)

(b)(7)(E)

The USAO (b)(6); (b)(7)(C) first became aware of the allegation concerning (b)(6); (b)(7)(C) after its review of the Verizon cell phone invoice for the billing cycle of (b)(6); (b)(7)(C) The invoice showed that (b)(6); (b)(7)(C) DOJ issued smartphone incurred $307.01 in data usage fees in (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C) also provided the OIG with a May 22, 2018 email he sent to all USAO (b)(6); (b)(7)(C) employees that outlined the requirements to seek approval to take DOJ issued cell phones when traveling internationally for either business or pleasure. The email's subject line read, "*Please Read - Foreign Travel with Government Issued Phones or BYOD Devices*" and the email read in part:

*Just a reminder, when traveling to foreign locations for work or for pleasure, you must seek approval (**at least 1 week prior to travel**) to bring your government issued iPhone.*

An OIG review of [redacted] DOJ email account identified a [redacted] email wherein [redacted] responded to [redacted] email. [redacted] wrote that he "was going to [redacted] in [redacted] but did not plan to take his DOJ issued smartphone and inquired how he could do work related conference calls from [redacted] due to "time-sensitive settlement negotiations." The OIG did not find a responsive email from [redacted] to [redacted] However, in [redacted] signed a "rules of behavior" document for cell phone users agreeing that iPhones must be approved by the United States Attorney or designee for international travel.

In a voluntary interview, [redacted] admitted he took his DOJ issued smartphone to [redacted] during his personal trip from [redacted] without proper DOJ authorization, and said he decided to do so at the last minute because he needed to stay involved in a rapidly developing high priority [redacted] case. [redacted] said he used "poor judgment" in taking his DOJ issued smartphone to [redacted] and that he was "pretty sure" there was an office policy regarding the need to obtain prior authorization to take his DOJ issued smartphone on international travel. [redacted] acknowledged his awareness of historical security concerns related to traveling to [redacted] with a DOJ issued cell phone and cited that as the reason he did not bring his DOJ issued cell phone to [redacted] in [redacted] [redacted] was not able to cite any changes in those concerns that occurred between [redacted]

[redacted] said he sent work related emails using his DOJ issued smartphone in [redacted] via non-DOJ approved data and Wi-Fi services but tried to minimize any potential threat by otherwise keeping the smartphone in airplane mode and in his possession at all times. [redacted] did not automatically turn in his DOJ issued smartphone to the USAO [redacted] upon his return from [redacted] on [redacted], but was instructed to do so at some point in [redacted]. [redacted] said that his DOJ issued smartphone was returned to him a short time later and appeared to have been "wiped." Approximately a few weeks later, [redacted] was again requested to turn in his DOJ issued smartphone to the USAO [redacted] and as of his OIG interview on [redacted] had not received a replacement DOJ issued cell phone.

[redacted] resigned from his position at the USAO effective [redacted]

[redacted]

OIG's Conclusion

The OIG investigation concluded that [redacted] transported his DOJ issued smartphone to [redacted] and used it during a personal trip there without DOJ authorization as alleged, and that his actions constituted administrative misconduct in violation of DOJ Order Number 0904: Cybersecurity Program, approved on September 15, 2016, DOJ Mobile Device and Mobile Application Security Supplement 2017 A, dated June 23, 2017, and USAPP, Version 1.1, #3-16-300-006, dated May 24, 2018.

[redacted]

(b)(6); (b)(7)(C)

[redacted]

(b)(6); (b)(7)(C)

[redacted]

(b)(6); (b)(7)(C)

[redacted]

(b)(6); (b)(7)(C)