

REPORT OF INVESTIGATION

SUBJECT [REDACTED] Trial Attorney [REDACTED]		CASE NUMBER [REDACTED]	
OFFICE CONDUCTING INVESTIGATION Washington Field Office		DOJ COMPONENT [REDACTED]	
DISTRIBUTION		STATUS	
<input checked="" type="checkbox"/> Field Office <input type="checkbox"/> AIGINV <input checked="" type="checkbox"/> Component <input type="checkbox"/> USA <input checked="" type="checkbox"/> Other OPR		<input type="checkbox"/> OPEN <input type="checkbox"/> OPEN PENDING PROSECUTION <input checked="" type="checkbox"/> CLOSED PREVIOUS REPORT SUBMITTED: <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO Date of Previous Report:	

SYNOPSIS

The Department of Justice (DOJ) Office of the Inspector General (OIG) initiated this investigation upon information received from the DOJ [REDACTED] alleging that during a routine security update, [REDACTED] staff discovered sexually explicit pictures and texts on Trial Attorney [REDACTED] government issued iPhone.

Following the initial referral, the OIG seized [REDACTED] DOJ issued laptop computer and iPhone.

The OIG investigation substantiated the allegation that [REDACTED] misused his DOJ issued iPhone and laptop computer by sending, receiving, and storing inappropriate explicit sexual images on both devices.

The OIG Cyber Investigation Office forensically reviewed data recovered from [REDACTED] DOJ issued laptop computer and DOJ issued iPhone. Both devices were found to contain sexually explicit material not associated with any official DOJ investigation or prosecutorial proceedings.

During a voluntary interview under oath, [REDACTED] admitted to using his government issued iPhone and laptop computer to transmit inappropriate explicit images of himself and receive inappropriate explicit images of multiple girlfriends over the past several years. He stated that he used his iPhone to send and receive the photographs because he did not own a personal iPhone.

DATE May 23, 2019	SIGNATURE [REDACTED]
PREPARED BY SPECIAL AGENT [REDACTED]	
DATE	SIGNATURE 
APPROVED BY SPECIAL AGENT IN CHARGE Russell W. Cunningham	

The OIG has completed its investigation and is providing this report to [REDACTED] and OPR 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).

DETAILS OF INVESTIGATION

Predication

The Department of Justice (DOJ) Office of the Inspector General (OIG) initiated this investigation upon information received from the DOJ [REDACTED], Washington D.C., alleging that during a routine security update, [REDACTED] staff discovered sexually explicit pictures and texts on Trial Attorney [REDACTED] government issued iPhone

Following the initial referral, the OIG seized [REDACTED] DOJ issued laptop computer and iPhone.

Investigative Process

The OIG's investigative efforts consisted of the following:

Interview of the following DOJ [REDACTED] personnel:

- [REDACTED] Trial Attorney

Review of the following:

- [REDACTED] DOJ issued iPhone
- [REDACTED] DOJ issued laptop computer

[REDACTED] Misuse of His Government Issued Laptop Computer and iPhone

The information provided to the OIG alleged that [REDACTED] violated DOJ policy by misusing his government issued iPhone to send, receive, and store sexually explicit material. A subsequent OIG forensic examination revealed [REDACTED] also misused his government issued laptop to send, receive, and store sexually explicit material.

[REDACTED] conduct violates DOJ policy. DOJ Order 2740.1A, Change 1, "Use and Monitoring of DOJ Computers and Computer Systems," Section 3c(2)(c), provides that users are prohibited from "The creation, download, viewing, storage, copying, or transmission of sexually explicit or sexually oriented materials or materials related to illegal gambling, illegal weapons, terrorist activities, and any other illegal activities." "The Rules for use of Tax Division iPhone" addendum states that employees must, "apply the same computer security guidelines to your iPhone."

The OIG Cyber Investigation Office (CYBER) reviewed the forensic images from [REDACTED] laptop and determined that [REDACTED] had sent or received mails with sexual content and without pictures from at least May 17, 2012, until August 26, 2016. One e-mail dated June 14, 2015 contained pornographic pictures. Approximately 180 pornographic pictures, dated from December 10, 2014, to December 17, 2016, were saved on [REDACTED] laptop.

Review of the forensic extraction from [REDACTED] iPhone determined that it contained approximately 150 pornographic pictures, dated from June 2, 2017, to December 31, 2017. There were also approximately 24 pornographic videos stored on [REDACTED] iPhone, dated from August 28, 2017, to December 23, 2017.

None of the women with whom [REDACTED] exchanged sexually explicit material were federal employees.

During his voluntary OIG interview, [REDACTED] admitted to using his government issued iPhone and laptop computer to send and receive explicit sexual images of himself and women he knew for the past several years. [REDACTED] told the OIG he did not perceive the pornographic photographs found on his DOJ devices as pornography, stating “I don’t consider them to be pornography, but that’s splitting hairs and I understand it and I perfectly well understand that I should have not had those images.”

[REDACTED] told the OIG that he understood DOJ rules of behavior and admitted that he violated DOJ policy by storing and transmitting sexually oriented material on his DOJ iPhone and laptop computer.

OIG’s Conclusion

The OIG investigation concluded that [REDACTED] did engage in misconduct as alleged, and that his actions violated DOJ Order 2740.1A, Change 1.