UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA,

Petitioner,

v.

Donna M. Hill,

Respondent.

Misc. No. 18-mc-00023 (TSC)

MEMORANDUM OPINION

Before the court are the United States' Petition and Amended Petition for Summary Enforcement of Inspector General Subpoena, and Respondent's Motion to Quash, or in the Alternative, for a Protective Order. For the reasons stated below, the court will GRANT in part and DENY in part the United States' petitions and Respondent's motion.

I. BACKGROUND

In January 2018, the United States Department of Justice Office of the Inspector General ("OIG") initiated an investigation into alleged misconduct by Federal Bureau of Prisons ("BOP") "employees in connection with a BOP contract award." ECF No. 2-1 (Declaration of Greg Thompson, "Thompson Decl.") ¶ 3. Pursuant to this investigation, the OIG requested that Respondent Donna M. Hill—an Executive Assistant at the BOP—produce the BOP-owned Samsung mobile telephone (hereinafter, "Samsung phone") and Microsoft Surface Pro Tablet (hereinafter, "Microsoft tablet") issued to her in connection with her employment. *Id.* ¶¶ 4, 6. The OIG has reason to believe that these electronic devices contain communications relevant to its investigation. *Id.* ¶ 5.

Despite the issuance of two administrative subpoenas requesting the immediate production of the Samsung phone and Microsoft tablet to the OIG, Respondent refused to produce the electronic devices, asserting that she was entitled to withhold the devices because personal information is stored on them. *Id.* ¶¶ 6, 7, 9, 16. She maintained this position even after the OIG sent an email to her counsel, explaining that the BOP warned her that she had no expectation of privacy while operating the electronic devices. *See id.* ¶ 10–13.

On February 16, 2018, the government filed a Petition for Summary Enforcement of Inspector General Subpoena, requesting that the court order Respondent to immediately produce the BOP-owned electronic devices pursuant to the OIG administrative subpoenas. ECF No. 1 (Gov't Pet.). A week later, the government filed a Motion for Temporary Restraining Order. ECF No. 2. Under the terms of the government's proposed temporary restraining order, Respondent would be required to immediately produce the BOP-issued devices, but the government would be prohibited from searching the devices until the government's Petition for Summary Enforcement was resolved or a search warrant was properly obtained. ECF No. 2-3 at 2. Respondent then filed a Motion to Quash, or in the Alternative, for Protective Order, arguing that because she has a constitutionally protected right to her personal information on the electronic devices, she did not have to comply with the OIG's subpoenas. ECF No. 5 (Respondent Mot.).

On March 16, 2018, this court entered a Temporary Restraining Order, concluding that (1) the United States was likely to succeed on the merits of its Petition for Summary Enforcement, (2) Respondent's continued withholding of the electronic devices would likely result in irreparable and serious damage to the OIG's investigation, (3) Respondent's alleged Fourth Amendment rights would not be violated as a result of a temporary restraining order because the OIG was

temporarily prohibited from searching the devices, and (4) the public interest favored entry of the Order. ECF No. 7 (TRO) at 3–4. The court ordered Respondent to immediately produce the Samsung phone and Microsoft tablet to Senior Special Agent Greg Thompson or any other OIG Special Agent. *Id.* at 4. The court also ordered the OIG to "refrain from taking any action with respect to the devices, including any action to physically or remotely search the devices or otherwise physically or remotely access the devices for any purpose" until further order of the court or until a search warrant was properly obtained. *Id.*

On April 27, 2018, the OIG learned that Respondent maintained possession of a third BOP-issued device—a Blackberry mobile telephone (hereinafter, "Blackberry"). ECF No. 17-1 (Second Supplemental Declaration of Greg Thompson, "Second Suppl. Thompson Decl.") ¶ 2. The OIG has reason to believe that the Blackberry also contains communications relevant to its investigation. *Id.* ¶ 4. Accordingly, on May 9, 2018, the OIG e-mailed a subpoena to Respondent's counsel—whom has maintained possession of the Blackberry since February 14, 2018—requesting production of the Blackberry "FORTHWITH." *Id.* ¶¶ 2–3.

Respondent refused to produce the Blackberry absent the OIG's agreement not to search it. *See* ECF No. 19 (Respondent Notice) at 1. Unwilling to enter into such an agreement, the government filed an Amended Petition for Summary Enforcement of Inspector General Subpoena and for Expedited Ruling. ECF No. 17 (Gov't Am. Pet.). In the Amended Petition, the government asks the court to order Respondent to produce her Blackberry and permit the government to search all three BOP-issued devices. *Id.* at 8. The parties rely on the briefing submitted in support of or in opposition to the government's initial Petition to Enforce (ECF No. 1) to support and oppose the Amended Petition. *See* ECF No. 16 (May 22, 2018 Order), *see also* Respondent Notice at 1, 3.

II. DISCUSSION

The court's role "in a proceeding to enforce an administrative subpoena is a strictly limited one." *FTC v. Texaco, Inc.*, 555 F.2d 862, 871–72 (D.C. Cir. 1977). The court is to determine whether "'the inquiry is within the authority of the agency, the demand is not too indefinite and the information sought is reasonably relevant'" to the agency's investigation. *United States Int'l Trade Comm'n v. ASAT, Inc.*, 411 F.3d 245, 253 (D.C. Cir. 2005) (quoting *United States v. Morton Salt Co.*, 338 U.S. 632, 652 (1950)). The subpoenaed party bears the burden of showing that the administrative subpoena is unreasonable; a burden "not easily met." *Texaco*, *Inc.*, 555 F.2d at 882.

Respondent does not contest the OIG's authority to issue the February and May 2018 subpoenas.[1] Therefore, the court focuses its analysis on the two remaining requirements of enforcement: that the requested information not be too indefinite and the information sought be reasonably relevant to the investigation.

A. The Subpoenas Are Not Too Indefinite

Respondent argues that the subpoenas are too indefinite because they "describe[] a general investigation into employee misconduct" and "[n]othing more." Respondent Mot. at 6. She further argues that the subpoenas fail to reveal whether she "is a 'subject,' 'target,' or 'witness'" in the investigation. *Id.* Because "there are no bounds, no direction and no limits to

[1] The Inspector General Act of 1978, 5 U.S.C. app. 3, as amended, authorizes the OIG to "subpoena the production of all information, documents, reports, answers, records, accounts, papers, and other data in any medium (including electronically stored information), as well as any tangible thing and documentary evidence necessary in the performance of the functions assigned by [the] Act." 5 U.S.C. app. 3 § 6(a)(4). One of the OIG's responsibilities is to detect fraud within the Department of Justice and its various components. *See* 5 U.S.C. app. 3 § 4(a).

the government's subpoena request[s]," Respondent argues, the subpoenas are unenforceable. *Id.* at 6–7. The court disagrees.

The OIG's subpoena requests are sufficiently defined and limited. They seek the production of three BOP-owned devices from one employee for one specific investigation: "an investigation into allegations of misconduct by an employee(s) of the Department of Justice." ECF No. 2-2; ECF No. 17-2 at 4. The information sought is limited to information generated on the three devices. Respondent cites no authority requiring that the subpoena be further limited or defined.[2] Absent such authority, the court is not inclined to require a more detailed subpoena, especially considering that "administrative investigatory subpoenas must by their very nature be broad." *United States v. Firestone Tire & Rubber Co.*, 455 F. Supp. 1072, 1083 (D.D.C. 1978); *see also Texaco, Inc.*, 555 F.2d at 882 ("There is no doubt that these subpoenas are broad in scope, but the FTC's inquiry is a comprehensive one and must be so to serve its purposes."); *Apodaca*, 251 F. Supp. 3d at 11 ("Yet, 'the boundary [of an investigation] may be defined quite generally' for the purposes of determining whether an administrative subpoena must be enforced.") (quoting *FTC v. Invention Submission Corp.*, 965 F.2d 1086, 1090 (D.C. Cir. 1992)). Accordingly, the court finds that the OIG's demands are not too indefinite.

[2] Respondent argues that "the government cites no relevant authority in which an administrative subpoena seeks such broad scale access to personal, private information as it does here." ECF No. 13 (Respondent Reply) at 6. However, in *United States v. Apodaca*, 251 F. Supp. 3d 1, 12 (D.D.C. 2017)—one of the cases on which the government relies—the court enforced subpoenas requiring the production of recorded jail calls for two defendants for a nearly two-year period of time. The recorded jail calls, similar to the BOP-owned devices at issue in this case, contained personal information. *See id.* at 6. Nonetheless, the court found that "the government [was] entitled to enforcement of the administrative subpoenas, and, thus, to the jail calls targeted therein." *Id.* at 12.

B. The Subpoenas Seek Relevant Information

A court "must enforce a federal agency's investigative subpoena if the information sought is reasonably relevant, or, put differently, not plainly incompetent or irrelevant to any lawful purpose of the agency, and not unduly burdensome to produce." *Invention Submission Corp.*, 965 F.2d at 1089 (internal quotation marks and citations omitted). Indeed, courts "defer to the agency's appraisal of relevancy, which must be accepted so long as it is not obviously wrong." *Resolution Trust Corp. v. Frates*, 61 F.3d 962, 964 (D.C. Cir. 1995) (quoting *Resolution Trust Corp. v. Walde*, 18 F.3d 943, 946 (D.C. Cir. 1994)). Given "the broad deference . . . afford[ed] the investigating agency, it is essentially the respondent's burden to show that the information is irrelevant." *Invention Submission Corp.*, 965 F.2d at 1090.

Respondent has failed to meet this burden. She has not argued that the information on the phones and tablet is "plainly incompetent or irrelevant to any lawful purpose of the agency" or that the information is "unduly burdensome to produce." *Id.* at 1089 (internal quotation marks and citations omitted). Nor has she argued that the agency's appraisal of relevancy is "obviously wrong." *Frates*, 61 F.3d at 964. Instead, Respondent generally asserts that enforcement of the subpoenas would grant OIG access to her "personal email, social media, location data, and internet search history," where personal, confidential communications are located. Respondent Reply at 4. These communications, Respondent argues, are of "dubious relevance" to the OIG's investigation into employee misconduct. Respondent Mot. at 6.

Respondent's general assertion of irrelevance is insufficient to outweigh the OIG's assertion that it "has reason to believe that [Respondent] has information relevant to the investigation, and has engaged in relevant communications using her BOP-issued devices." Thompson Decl. ¶ 5. It is not "obviously wrong" that these relevant communications and

information could be contained in Respondent's personal email, social media accounts, location data, or internet search history. Accordingly, the court finds that information contained on the BOP-owned devices—whether contained in personal accounts or elsewhere—is reasonably relevant to the OIG's investigation.

C. The Subpoenas Do Not Violate the Fourth Amendment

Respondent argues that enforcement of the OIG's subpoenas would violate her Fourth Amendment rights. Specifically, she argues that she has a reasonable expectation of privacy in "her personal information stored on the devices and in the cloud," Respondent Mot. at 12, and that enforcement of the subpoenas would provide the OIG improper access to this information. This argument is also unavailing.

The Fourth Amendment "'guarantees the privacy, dignity, and security of persons against certain arbitrary and invasive acts by officers of the Government.'" *City of Ontario, Cal. v. Quon*, 560 U.S. 746, 755–56 (2010) (quoting *Skinner v. Railway Labor Executives' Assn.*, 489 U.S. 602, 613–14 (1989)). It is recognized that "'the touchstone of Fourth Amendment analysis is whether a person has a constitutionally protected reasonable expectation of privacy.'" *Stewart v. Evans*, 351 F.3d 1239, 1243 (D.C. Cir. 2003) (quoting *California v. Ciraolo*, 476 U.S. 207, 2011 (1986)). However, "[t]o the extent the Fourth Amendment is implicated by the use of an administrative subpoena, satisfaction of [the authority, definiteness, and relevance] requirements also satisfies that amendment." *Apodaca*, 251 F. Supp. 3d at 8. Because the OIG was authorized to issue the subpoenas, and the subpoenas are sufficiently definite and relevant to the OIG's investigation into potential contract fraud, the court finds that the OIG's subpoenas satisfy the Fourth Amendment.

Even assuming *arguendo* that a reasonable expectation of privacy determination is

warranted in this case, Respondent has failed to establish such a reasonable expectation. As an initial matter, the cases upon which Respondent relies do not support her assertion that she—a BOP employee—has a reasonable expectation of privacy in the personal information stored on the BOP-issued devices. Indeed, *Riley v. California*, 134 S. Ct. 2473 (2014), and *United States v. Jones*, 565 U.S. 400 (2012), both involved the defendants' privacy interests in *personally-owned* devices, and therefore provide no guidance for this court's determination as to whether Respondent has a reasonable expectation of privacy with respect to the three *government-owned* devices at issue. *Riley*, 134 S. Ct. at 2481 (personal cell phone searched incident to arrest); *Jones*, 565 U.S. at 402 (GPS device attached to a personal vehicle in a criminal investigation).

Additionally, in *Quon*, although the Supreme Court declined to rule broadly on the privacy expectations a government employee may have in government-issued electronic devices, the Court noted that when a government employee is told that an electronic device is "subject to auditing," he should be on notice that a search may take place. 560 U.S. at 763 ("Even if he could assume some level of privacy would inhere in his messages, it would not have been reasonable for Quon to conclude that his messages were in all circumstances immune from scrutiny. Quon was told that his messages were subject to auditing. As a law enforcement officer, he would or should have known that his actions were likely to come under legal scrutiny, and that this might entail an analysis of his on-the-job communications."). Thus, not only do *Riley*, *Jones*, and *Quon* not support Respondent's contention that she "has a reasonable expectation of privacy in her personal information housed on the [BOP-owned] devices," Respondent Mot. at 7, but *Quon* suggests that the opposite may be true.

Moreover, as in *Quon*, Respondent was informed that she had no reasonable expectation of privacy in the information stored on the phones and tablet. Specifically, the BOP Office of

Information Technology's Samsung S7 policy handbook—which Respondent received along with her Samsung phone—states: "[i]f personal information is stored on the device, it may be subject to search and production due to e-Discovery/litigation, FOIA requests, or an *administrative staff investigation*." ECF No. 5-2 (BOP Samsung Galaxy S7 Policy) at 42 (emphasis added). And when Respondent initially activated her BOP-issued Samsung phone, she was required to confirm her receipt and understanding that the Samsung phone is "a Government furnished device and [that] all activities may be monitored." *Id.* at 15; ECF No. 11-1 (Supplemental Declaration of Greg Thompson, "Thompson Suppl. Decl.") ¶ 2.

Further, each time Respondent logged onto her BOP-issued Microsoft tablet or BOP-issued desktop computer, she received the following warning:

> You have no reasonable expectation of privacy regarding any communications transmitted through or data stored on this information system. At any time, the government may monitor, intercept, search and/or seize data transiting or stored on this information system.

Thompson Dec. ¶ 11; Thompson Supp. Decl. ¶ 3. This warning made clear that the "information system" included "(1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network." *Id.* By the warning's express terms, all three BOP-owned devices—Samsung phone, Microsoft tablet, and Blackberry—are "attached" to the BOP network, and therefore are connected to the BOP information system and may be subject to search. Thompson Supp. Decl. ¶ 4; Thompson Second Supp. Decl. ¶ 6.

Notwithstanding these warnings, Respondent maintains that she reasonably believed that the "personal business [she] conducted while . . . not connected to the BOP network would remain private." ECF No. 13-1 (Respondent Decl.) ¶ 7. In her declaration, she explains that both

the Microsoft tablet and the Samsung phone enabled her to communicate and send documents outside of the BOP network. Once logged onto the Microsoft tablet, Respondent explains, she was able to either log in securely to the BOP network through a VPN connection via the "Cisco" application or she could conduct personal business on the tablet, unconnected to the BOP network. *Id.* ¶¶ 6–7. Respondent further explains that the Samsung phone has a "Knox Workspace" and a "Personal Space"—both of which require a different password.[3] *Id.* ¶¶ 9–10. Respondent was only able to connect to the BOP network through the "Knox Workspace;" she conducted all "personal business" in the "Personal Space." *Id.* ¶¶ 10–11. Respondent maintains that it was her understanding that only those communications and documents transmitted while connected to the BOP network were monitored or subject to a search. *Id.* ¶¶ 7, 11. She believed that those communications and documents transmitted outside the network would remain private. *Id.*

However, as explained previously, BOP's policies make clear that all three BOP-owned devices are—in their entirety—a part of the "information system" because they are "attached to [the BOP] network." Thompson Supp. Decl. ¶ 4; Thompson Second Supp. Decl. ¶ 6. While it is true that one can operate the devices without connecting to the BOP network, the devices themselves are attached to the network, and are therefore subject to monitoring, searching and seizure. Respondent was not informed otherwise. Thompson Supp. Decl. ¶ 6 ("The BOP has never provided assurance of privacy to any user of Government Furnished Equipment (GFE)."); *see also* Thompson Second Supp. Decl. ¶¶ 8–9. Like the government employee in *Quon*,

[3] According to the OIG, the "Knox Workspace on the BOP-issued Samsung mobile device is an on-device container that isolates business applications from personal ones with government-grade security to enable the government to protect against compromises to the BOP network that could originate in personal use applications such as email." Thompson Supp. Decl. ¶ 7.

Respondent "should have known that [her] actions were likely to come under legal scrutiny." 560 U.S. at 762. Accordingly, the court finds that Respondent had no reasonable expectation of privacy in her personal information on the three BOP-owned electronic devices.

D. Respondent's Privileged Communications with Counsel Must Be Protected

In a footnote, Respondent argues that because the BOP-issued Samsung phone "contains privileged communications with counsel, any ruling in favor of the government should include the requirement that a taint team be assembled to ensure that [her] privilege is maintained." Reply at 4 n.3. Respondent does not provide any detail regarding the extent to which she used the BOP-owned devices to communicate with her attorneys. Nor does Respondent provide the court with a proposed order, describing the mechanisms the OIG should implement to ensure that Respondent's attorney-client privilege is maintained during its search of the electronic devices. Respondent also fails to cite any authority for her proposition that the court should require the assembling of a "taint team" prior to allowing the OIG to search the Samsung phone.

Nonetheless, the court finds that, even in the context of enforceable administrative subpoenas, the subpoenaed party is entitled to the protection of her privileged communications with counsel. *See FTC. v. Boehringer Ingelheim Pharmaceuticals, Inc.*, 778 F.3d 142, 158 (D.C. Cir. 2015) (ordering the district court to determine whether the attorney-client privilege barred discovery sought pursuant to an administrative subpoena); *see also SEC v. Karroum*, 2015 WL 8483246, at *4 (D.D.C. Dec. 9, 2015) (enforcing an administrative subpoena and finding that the respondent's "attorney-client and marital privileges will be properly protected by means of the privilege-review procedure"). Accordingly, the court will order the parties to submit a proposed protective order within five days of this decision that addresses Respondent's attorney-client privilege concerns. Additionally, the court will order Respondent to produce the Blackberry

device and will order the OIG to refrain from searching all three devices until the court has issued the protective order.

III. CONCLUSION

For the foregoing reasons, (1) the United States' Petition for Summary Enforcement of Inspector General Subpoena, (2) the United States' Amended Petition for Summary Enforcement of Inspector General Subpoena and (3) Respondent's Motion to Quash, or in the Alternative, for a Protective Order will all be GRANTED in part and DENIED in part.

A corresponding order will issue separately.

Date: June 20, 2018

Tanya S. Chutkan
TANYA S. CHUTKAN
United States District Judge