

SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF NEW YORK

-----X
In re Application for a Judgment under Article 78 of
the Civil Practice Law and Rules by

SUSAN CRAWFORD,

Petitioner,

Index No. 157002/2015
IAS Part 6
(Lobis, J.)

-against-

NEW YORK CITY DEPARTMENT OF
INFORMATION TECHNOLOGY
TELECOMMUNICATIONS,

Respondent,

AND

AT&T CORP., EMPIRE CITY SUBWAY COMPANY
LTD., TIME WARNER CABLE INC., and RCN
TELECOM SERVICES, LLC.,

Intervenors-Respondents.

-----X

**MEMORANDUM OF LAW IN SUPPORT OF
RESPONDENT NEW YORK CITY
DEPARTMENT OF INFORMATION
TECHNOLOGY TELECOMMUNICATIONS'
VERIFIED ANSWER**

PRELIMINARY STATEMENT

This memorandum of law is submitted on behalf of Respondent New York City Department of Information Technology Telecommunications (“DoITT”) in support of its Verified Answer to the Verified Petition in this Article 78 proceeding, brought pursuant to New York State’s Freedom of Information Law (“FOIL”).

This proceeding is Petitioner’s second attempt to compel DoITT to disclose highly sensitive information regarding New York City’s subsurface conduit infrastructure, which houses the cables that provide Internet and telecommunication services to individuals, government agencies, and other entities throughout the City and to certain parts of the world.

Petitioner's first attempt to obtain this information was rejected in *Crawford v. N.Y.C. Dep't of Info. Tech. & Telecom.*, 982 N.Y.S.2d 725 (Sup. Ct., N.Y. Co. 2014) ("*Crawford I*"). In that case, the Court held that the infrastructure information Petitioner sought was exempt from disclosure pursuant to Public Officers Law § 87(2)(i) (the "infrastructure exemption"), which permits an agency to deny access to records that would jeopardize its ability to guarantee the security of its information technology assets.

As further explained below, the information Petitioner seeks in this proceeding is nearly identical to the information that was protected from disclosure in *Crawford I* and thus falls squarely within FOIL's infrastructure exemption. The information is additionally exempt from disclosure because its release could endanger the lives and safety of individuals in New York City, *see* Public Officers Law § 87(2)(f) (the "life/safety exemption"), and would substantially injure the competitive position of businesses that lease space in the conduits, *see* Public Officers Law § 87(2) (d) (the "trade secret" exemption"). The Verified Petition should accordingly be denied in its entirety.

STATEMENT OF FACTS

A. New York City's Conduit Infrastructure

The subject of this proceeding is a spreadsheet prepared by Intervenor-Respondent Empire City Subway ("ECS"), which contains detailed information about New York City's subsurface electrical conduit infrastructure.

The City's conduit infrastructure consists of 58 million feet of conduits connected within approximately 11,000 manholes; both the conduits and manholes are maintained by ECS. *See* Verified Answer ¶¶ 31, 37, 38. The conduits are physical tubes that protect and route the copper, coaxial and fiber-optic telecommunications cables that carry voice telephone, cable television and Internet services to millions of residents and businesses in the City, public and

private hospitals, financial institutions, the State and federal court systems, and critical government agencies, such as the New York City Police Department (“NYPD”) and the New York City Fire Department (“FDNY”). *Id.* at ¶¶ 32-33. The manholes, which are visible at the street level, serve as access points to the conduits and cables and enable workers to route the cables in various directions. *Id.* at ¶ 37.

Government and law enforcement agencies rely on the cables within the conduit infrastructure to communicate vital information to the public, respond to emergencies, and perform other essential services. *Id.* at ¶ 34. Because the cables run just underneath City streets, they are extremely vulnerable to physical damage, such as by cutting, melting, and other acts of vandalism. *Id.* at ¶ 36.

B. *Crawford I*: Petitioner’s Previous Attempt to Compel Production, through FOIL, of Information regarding the City’s Conduit Infrastructure

In January 2012, Petitioner submitted a FOIL request to DoITT seeking, among other things, all records concerning the geographic location of conduits owned and operated by ECS. *See Crawford I*, 982 N.Y.S.2d at 738. The records responsive to the request consisted of 41 maps depicting the geographical locations of the City’s conduits and the cables within those conduits. *Id.* at 742. DoITT determined that disclosure of the maps (i) would jeopardize its ability to guarantee the security of the conduits and the cables within them, and (ii) could endanger the lives and safety of individuals in New York City. It accordingly denied Petitioner’s FOIL request for the maps pursuant to FOIL’s infrastructure and life/safety exemptions set forth in Public Officers Law §§ 87(2)(i) and (f).

Petitioner then commenced an Article 78 proceeding against DoITT, seeking judicial review of DoITT's determination to withhold the maps and production of the maps. *Crawford I*, 982 N.Y.S.2d at 742. In opposition to the petition and in support of its answer to uphold its determination, DoITT submitted the affidavit of Sergeant Martin Wingert, an engineer and supervisor at the NYPD's Counterterrorism Division Threat Reduction Infrastructure Protection Section. Sergeant Wingert reviewed the maps and concluded that "public dissemination of [the] maps would put New York City's electronic information infrastructure at risk." *Id.* at 742 (internal quotations omitted). Specifically, Sergeant Wingert explained that because the maps depicted the City's conduit infrastructure and corresponding fiber optic network in great detail, the maps could be used to orchestrate attacks on the conduits and cables, which in turn could compromise the ability of the government to perform its essential services, including NYPD's ability to provide security to the City's residents. *Id.* at 742.

By Decision and Order dated March 20, 2014, Justice Shlomo Hagler denied the petition in *Crawford I*. *Id.* at 743, 744-45. Deferring to Sergeant Wingert's professional expertise on the matter, Justice Hagler held that "disclosure of the precise information on the maps would [...] jeopardize [the City's] ability to guarantee the security" of its conduits and that the maps were accordingly properly withheld from disclosure under FOIL's infrastructure exemption.

C. *Crawford II: Petitioner's Second Attempt to Compel Production, through FOIL, of Information regarding the City's Conduit Infrastructure*

i. *The FOIL Request Underlying this Proceeding and DoITT's Response*

Several months later, by letter dated May 9, 2014, Petitioner submitted another FOIL request to DoITT seeking, among other things, "records sufficient to disclose [...] the total number of conduits owned or operated by ECS, broken down by the smallest geographic unit available to DoITT (e.g. zipcode, neighborhood, block or similar defined region)." *See* Verified Petition, Exhibit A. In response to this request, DoITT produced, by letter dated January 30, 2015, a spreadsheet that had been provided to it by ECS. *See* Verified Petition, Exhibits G and H.

The spreadsheet consists of several worksheets that show each segment in the City's conduit infrastructure, the geographic location of the manhole at the start and end point of each conduit segment, the identity of the tenants occupying each conduit segment, and the ducts and number of ducts occupied by the tenants in each conduit segment. *See* Verified Petition, Exhibit G. A separate worksheet in the spreadsheet contains an alphabetical list of each tenant that occupies space in the conduits. *See id.* Before producing the spreadsheet, DoITT redacted (i) the geographic location of the manholes associated with each conduit segment, (ii) the identity of the tenants occupying each conduit segment, and (iii) the alphabetical list of tenants occupying the conduits. *See* Verified Answer ¶ 46.

In its production letter, DoITT explained that the manhole location information was exempt from disclosure pursuant to FOIL's infrastructure exemption, and that the tenant information was exempt under FOIL's trade secret exemption. *See* Verified Petition, Exhibit H.

ii. Petitioner's Appeal of DoITT's Response and DoITT's Final Determination

By letter dated February 26, 2015, Petitioner appealed DoITT's redactions of the geographic location of the manholes as "overly broad" and "not authorized by any FOIL exemption." *See* Verified Petition, Exhibit I. Petitioner argued that disclosing the locational information "in whole or in part, would not raise security concerns over access to electronic information systems and infrastructures of the narrow type covered by [the claimed] exemption" and that disclosing the manhole locations themselves would not reveal the path of the conduits. *See id.* Petitioner also appealed DoITT's redaction of the names of the tenants using each conduit and the redaction of the alphabetical list of tenant names, arguing that disclosure of such information would not result in substantial harm to the tenants. *See id.*

DoITT partially denied Petitioner's appeal by letter dated March 12, 2015. *See* Verified Petition, Exhibit J. DoITT responded to Petitioner's argument that the manhole location information was not protected from disclosure under the infrastructure exemption as follows:

As you are aware, you previously sought production of maps showing the location of ECS conduit[s]. DoITT denied your request pursuant to [the infrastructure exemption], and that denial was sustained in [*Crawford I*]. The conduit location information on the unredacted spreadsheet is no less sensitive than the conduit location information on the maps, and therefore the [*Crawford I*] case is dispositive.

See id.

Next, in response to Petitioner's claim that disclosure of the manhole locations would not reveal precise information about the path of the conduits, DoITT stated:

I disagree in two respects. First, because conduits connect to manholes, disclosure of manhole locations would itself disclose conduit locations. Second, while disclosure of manhole locations would leave some degree of uncertainty about the location of conduit between manholes, that uncertainty in most cases would be a matter of no more than a few feet - about the same level of uncertainty as for the maps. Thus the manhole locations sufficiently describe the pathways of conduit between manholes as to expose the risk identified by the [*Crawford I*] court.

See id.

In response to Petitioner's appeal of the redacted customer names, DoITT partially granted the appeal by producing the worksheet that contained an alphabetical list of the tenants occupying the conduits. *See id.* DoITT did, however, uphold its determination to redact the identities of the tenants associated with each conduit segment pursuant to FOIL's trade secret exemption. *See id.*

iii. The Present Proceeding

Petitioner then initiated the instant Article 78 proceeding in July 2015 to compel DoITT to disclose the redacted portions of the spreadsheet. *See Verified Petition at p. 6.*

D. The NYPD's Assessment of the Risks Posed by Disclosure of the Information Petitioner seeks regarding the City's Conduit Infrastructure

After Petitioner commenced this proceeding, the Chief of the NYPD's Counterterrorism Bureau James Waters reviewed the unredacted spreadsheet. *See* accompanying Affidavit of James Waters, dated February 3, 2017 ("Waters Aff.") at ¶ 7. The Counterterrorism Bureau is tasked with enhancing the security of New York City and guarding against the threat of international and domestic terrorism in New York City. *Id.* at ¶ 3. Chief Waters has been the Bureau's highest-ranking official since 2008 and has over 36 years of law enforcement experience. *Id.* at ¶ 6.

According to Chief Waters, the unredacted spreadsheet could provide terrorists with "critical intelligence" to carry out physical and/or cyber-attacks on the City's information infrastructure. *Id.* at ¶ 15, 36. In his affidavit, Chief Waters explains that the unredacted spreadsheet "does not require any special training or skills to decipher" and "can be used to easily create a map of the City's electrical conduits and corresponding fiber optic networks." *Id.* at ¶¶ 18-19.

Furthermore, the map that can be created from the spreadsheet would "largely be the same" as the maps that were at issue in *Crawford I*. *Id.* at ¶¶ 19-20. That is, the map would (i) show the geographical location of the conduits, give or take a few feet; (ii) reveal the routing framework of fiber optic cables under the City's streets; (iii) reveal critical data transit points and the most vulnerable areas in the conduits; and (iv) indicate the means of accessing those points and conduits. *Id.* at ¶¶ 19-21. In other words, disclosure of the unredacted spreadsheet would pose the same risk of physical and cyber-attacks that disclosure of the maps in *Crawford I* posed. *Id.* at ¶ 13-14 and Exhibit A.

In terms of a physical attack, Chief Waters asserts that a malicious actor can use the map derived from the spreadsheet to determine which conduits and cables to vandalize to create targeted disruption of Internet and voice communications in the City and which manholes to enter to access those conduits and cables. *Id.* at ¶ 25-26. The map can also be used to “identify means to [REDACTED] [REDACTED].” *Id.* at ¶ 26. Damage to “one or two” strategic cables “could result in system-wide disruptions” in the City and other parts of the world that could place “countless lives at risk.” *Id.* at ¶ 27. However, Chief Waters notes that even a “small-scale, unsophisticated attack could be calamitous” as it would affect civilians’ ability to make 911 calls, “drastically increase emergency response times, and make it nearly impossible for government agencies, such as the NYPD and FDNY, as well as public and private hospitals, to communicate effectively in an emergency.” *Id.* at ¶ 28. A physical attack could also result in significant economic loss by disrupting the stock exchange and communications by and between financial institutions that rely on high-speed telecommunication services to transact business. *Id.* at ¶ 29. A physical attack on fiber optic networks is more than a hypothetical threat. *Id.* at ¶ 35. As Chief Waters explains in his affidavit, between June 2014 and September 2015, unknown perpetrators cut at least 16 fiber optic cables in the San Francisco Bay area of California, causing disruptions in the area’s essential emergency communications and Internet service. *Id.*

In terms of a cyber-attack, Chief Waters explains that a malicious actor can use fields in the spreadsheet to identify specific vulnerabilities in a network for exploitation and [REDACTED] [REDACTED].” *Id.* at ¶ 32. The actor can also devise means to [REDACTED]

[REDACTED]. *Id.* at ¶ 33. Such eavesdropping can lead to the “disclosure of public safety data or other sensitive data, which can then be exploited to further compromise the networks of the NYPD and other local, State, and federal governmental agencies, as well as public utilities.” *Id.* at ¶ 32. Cyber-attacks could also be used to invade ordinary residents’ personal privacy, and information gleaned from such attacks could be used for blackmail and/or ransom. *See id.* at ¶ 34.

In light of the foregoing risks, the fact that the City’s residents and government agencies rely on the conduit infrastructure to communicate effectively during emergencies, *see id.* at ¶ 22, and the fact that New York City’s infrastructure is a “high value target for terrorist organizations” and consistently targeted by terrorists, *see id.* at ¶ 39 and Exhibit B, Chief Waters concluded that disclosure of the unredacted spreadsheet would (i) subject the City’s infrastructure to an “unacceptable level of vulnerability,” (ii) “unquestionably” compromise the safety of the City of New York and its residents, and (iii) “run[]contrary to the highest priority of preventing another large-scale, mass casualty attack in New York City,” *see id.* at ¶¶ 24, 36, 40.

ARGUMENT

Any person denied access to a record or portion of a record by a government agency may, after exhausting her administrative remedies, seek judicial review of the denial by bringing a proceeding under Article 78 of the Civil Practice Law and Rules. To defend the denial of access, the agency must articulate a “particularized and specific justification” for not disclosing the requested information. *Gould v. N.Y.C. Police Dep’t*, 89 N.Y.2d 267, 275 (1996). If a court can determine that the withheld information falls within the scope of an allowed exemption, it should uphold the agency’s determination. *Id.*

Petitioner here seeks judicial review of DoITT's decision to redact (i) the locations of manholes that connect New York City's subsurface conduit segments, and (ii) the identities of the tenants occupying each conduit segment. Petitioner also seeks to compel production of the redacted information. This Court should uphold DoITT's redactions because they were properly made pursuant to FOIL's (i) infrastructure exemption, (ii) life/safety exemption, and (iii) trade secret exemption.¹ See Public Officers Law § 87(2)(i), (f) and (d).

POINT I

**DOITT PROPERLY REFUSED TO DISCLOSE
THE PRECISE LOCATIONS OF MANHOLES
CONNECTING CONDUITS BECAUSE SUCH
DISCLOSURE WOULD JEOPARDIZE THE
SECURITY OF NEW YORK CITY'S
INFORMATION INFRASTRUCTURE**

Public Officers Law §87(2)(i) permits an agency to withhold records that, "if disclosed, would jeopardize the capacity of an agency or an entity that has shared information with an agency to guarantee the security of its information technology assets, such assets encompassing both electronic information systems and infrastructures." This exemption is "concerned with ensuring the security of information technology assets." *Matter of TJS of N.Y. v. New York State Dep't of Taxation & Fin.*, 89 A.D.3d 239, 243 (3d Dep't 2011). The security consideration extends to both "electronic data and the physical system or infrastructure that carries [such] data." *Crawford I*, 982 N.Y.S.2d at 741. To withhold information pursuant to the infrastructure exemption, an agency must show (i) that the withheld information depicts "electronic information systems" or "infrastructures," and (ii) that disclosure of the withheld

¹ This Memorandum addresses only the first two exemptions. The applicability of the third exemption is explained by the memorandum submitted by Intervenor-Respondents AT&T Corporation, Time Warner Cable Inc., and RCN Telecom Services, LLC in opposition to the Verified Petition. See Docket No. 141. These Intervenor-Respondents are among the service providers whose competitive position would be injured by disclosure of the information Petitioner seeks.

information “would jeopardize the [agency’s] ability to ‘guarantee the security of its information technology assets.’”

Crawford I is directly on point. In that case, Petitioner Crawford and another petitioner sought to compel DoITT to produce maps that showed the geographic location of the conduits owned and operated by ECS. 982 N.Y.S.2d 725, 741. DoITT denied the request based on the infrastructure exemption and the Court upheld the denial. First, the Court held that New York City’s underground conduits “come within the purview of electronic information systems and infrastructures” protected by Public Officers Law § 87(2)(i). Second, the Court found, based on information provided by Sergeant Martin Wingert of the Counterterrorism Bureau, that disclosure of the precise information of the conduits on the maps “would pose a substantial threat” to the City’s information infrastructure and “would jeopardize [DoITT’s] ability to guarantee the security of its information technology assets.” *Id.* at 743 (internal quotations omitted).

In finding the information technology exemption applicable, the Court credited Sergeant Wingert’s assertions (i) that “[k]nowledge of the precise location of the conduits would help an attacker disrupt communications and data flowing through such conduits” (ii) that “even a single attack on a remote location could cause a ‘substantial disruption or interruption’ of computers that could compromise the ability of government to perform its essential services” (iii) that “a more precisely targeted attack on certain cables ‘could result in an internet disruption not only in New York City but also throughout the Unites States and overseas’”; and (iv) that the effects of these attacks “could lead, among other terrible scenarios, to impede the ability of police to communicate and provide security, and to delete valuable data in government and the private sector.” *Id.* at 741-43.

This Court should similarly find FOIL's infrastructure exemption applicable to the unredacted spreadsheet Petitioner seeks in this case. First, as the unredacted spreadsheet can be used to easily create a map of the City's conduits, which under *Crawford I* constitutes "electronic information systems and infrastructures," the spreadsheet meets the first element of the exemption. Indeed, the requested information is simply another permutation of the map that was exempt from disclosure in *Crawford I*. See *Waters Aff.* ¶¶ 13, 19-20. The information also meets the second element of the exemption because disclosure of the unredacted spreadsheet would expose highly detailed information about the City's conduit infrastructure and thus subject the infrastructure to an "unacceptable level of vulnerability." See *Waters Aff.* ¶¶ 24, 36. Specifically, the unredacted spreadsheet would allow an individual to (i) easily create a geographically accurate map of the City's conduit infrastructure and its corresponding fiber optic network and (ii) identify critical data transit points and the most vulnerable areas in the conduits, and (iii) determine remote means of accessing those points and conduits. The individual could then use the information derived from the spreadsheet to tailor physical and cyber-attacks on the City's infrastructure and evade detection.

This Court should defer to Chief Waters' professional judgment that disclosure of the unredacted spreadsheet will jeopardize the City's ability to protect its infrastructure from attack. As the highest-ranking official in the NYPD's Counterterrorism Bureau, Chief Waters' expertise in this area is unparalleled. Further, as the Second Circuit has recognized, "it is bad law and bad policy to second-guess the predictive judgments made by the government's intelligence agencies regarding whether disclosure of the information [...] would pose a threat to national security." *American Civ. Liberties Union v Department of Justice*, 681 F3d 61, 70-71 (2d Cir. 2012) (internal quotations omitted).

Petitioner's assertions that DoITT could unredact manhole location information in the spreadsheet for areas that are underserved and "removed from high risk targets" without jeopardizing the safety of the conduit infrastructure is flawed in at least three respects. *See* Pet.'s Memorandum (Docket No. 3) at pp. 12-13, 15-17. First, underserved areas are no less entitled to protection than other areas of New York City. Releasing information about certain neighborhoods will unacceptably jeopardize the safety of the infrastructure in those areas, and concomitantly subject individuals in those areas to a heightened threat of losing access to Internet and voice communications, which in turn, will endanger their timely access to critical emergency services, such as those provided by 911, the NYPD, and hospitals. Second, the City's conduit infrastructure is highly interconnected, thus disclosing specific information about the infrastructure in one area will unnecessarily jeopardize the safety of the entire structure. Third, the City is in a constant flux of development, and areas allegedly "removed from high risk targets" today may house high risk targets in the future.

In sum, DoITT properly withheld the unredacted spreadsheet because, like the maps at issue in *Crawford I*, the unredacted spreadsheet reveals highly-sensitive and detailed information about the City's conduit infrastructure, and disclosure of the information would unquestionably jeopardize the City's ability to guarantee the safety of the conduits from physical and cyber- attacks. *See* Waters Aff. ¶¶ 13, 15, 21, 32, 36, 40.

POINT II

**DOITT PROPERLY REFUSED TO DISCLOSE
THE PRECISE LOCATIONS OF MANHOLES
CONNECTING CONDUITS BECAUSE SUCH
DISCLOSURE COULD ENDANGER THE
LIVES AND SAFETY OF MANY PEOPLE**

Under Public Officers Law § 87(2)(f) (“life/safety exemption”), an agency may deny access to records or to portions thereof where the information, if disclosed, could endanger the life or safety of any person. The agency is not required to prove that a danger to a person’s life or safety will occur if the information is made public. *See Stronza v. Hoke*, 148 A.D.2d 900, 900-01 (3d Dep’t 1989) (citing *Nalo v. Sullivan*, 125 A.D.2d 311 (2nd Dep’t 1986)). Instead “there need only be a *possibility* that such information would endanger the lives or safety of individuals.” *Id.* (emphasis added).

Rankin v. Metropolitan Transit Authority is instructive. There, petitioners commenced an Article 78 proceeding to compel the Metropolitan Transit Authority (“MTA”) to release blueprint maps of all New York City subway stations. 2010 N.Y. Misc. LEXIS 3829 (Sup. Ct., N.Y. Co. Aug. 10, 2010). In opposing the motion, respondent submitted affidavits from, among others, the NYPD’s Counterterrorism Division. The Court found that the MTA properly invoked the life/safety exemption and was within its rights to withhold the blueprint maps because the NYPD had demonstrated how “disclosure could have potentially devastating effect by making available to potential terrorists highly sensitive material concerning structural details of the stations [...] and other information which would enhance the ability of such terrorist to maximize the damage to the NYCTA subway system and increase the loss of lives.” *Id.* at *13-14. The Court further found that “the danger posed to the life and safety of riders and NYCTA employees is more than just speculative, but rather, based upon the number of terrorist

attacks that have targeted transit systems around the world in recent years, is a very real and potential danger that far outweighs petitioner's right to access." *Id.* at *13-14.

Similarly, the information Petitioners seek in this proceeding is exempt from disclosure under FOIL's life/safety exemption.² As Chief Waters explained in his Affidavit, New York City's infrastructure has been repeatedly subject to attacks and plots over the past several years and remains a high-value target for potential terrorist attacks. *See Waters Aff.* at ¶¶ 37-38 and Exhibit B. Disclosure of the redacted information could jeopardize the safety and security of the residents of New York City and would unacceptably increase the risk of another terrorist attack. *Id.* at ¶¶ 15, 21, 25, 36. Specifically, the redacted information could be used to determine which cables to sever or damage in order to create system-wide disruptions, which would "drastically increase emergency response times, and make it nearly impossible for government agencies, such as the NYPD and FDNY, as well as public and private hospitals, to communicate effectively in an emergency." *Id.* at ¶ 28.

² DoITT did not raise this exemption in its response to Petitioner's FOIL request or its final determination. However, because Petitioner seeks both judicial review of DoITT's redactions *and* an order directing DoITT to disclose the redacted information, this proceeding is both a review of an administrative determination *and* a mandamus to compel. The Court is accordingly not limited to merely reviewing the exemptions DoITT raised in the administrative proceeding and "may consider additional grounds for denial of disclosure not raised at the administrative level." *See, e.g. Collins v. New York City*, 2013 NY Slip Op 30032(U), ¶ 7 (Sup. Ct., N.Y. Co. Jan. 9, 2013), *rev'd on other grounds*, 2013 N.Y. Misc. LEXIS 4729 (Sup. Ct., N.Y. Co. Oct. 16, 2013); *Greene v. City of N.Y.*, 763 N.Y.S.2d 880, 884 (Sup. Ct., N.Y. Co. 2003).

The resulting threat to the safety and security of individuals in New York City is self-evident. Individuals in need of assistance from police officers, the fire department, and hospitals may experience a lag in response time, which could be the difference between life and death. The redacted information could also be used to determine which cables to tap in order to eavesdrop on highly-sensitive information, including information circulated by and between law enforcement agencies. *Id.* at ¶ 32. Such information can in turn be exploited by terrorists to evade detection and carry out attacks. *Id.* at ¶¶ 15, 32.

This Court should accordingly find that the unredacted spreadsheet is exempt from disclosure under FOIL's life/safety exemption. *See, e.g., Grabell v. N.Y.C. Police Dep't.*, 32 N.Y.S.3d 81, 84 (1st Dep't 2016) (finding records exempt under life/safety exemption based on affidavit by NYPD's Deputy Commissioner of Counterterrorism, who averred that disclosure of the records would "hamper NYPD's counterterrorism operations" and "increase the likelihood of another terrorist attack"); *Asian Am. Legal Def. & Educ. Fund v. N.Y.C. Police Dep't.*, 5 N.Y.S.3d 13, 15 (1st Dep't 2015) (finding records exempt under life/safety exemption where requested records, which "could be [...] potentially exploited by terrorists, would create 'a possibility of endangerment'").

POINT III**PETITIONER IS NOT ENTITLED TO ATTORNEYS' FEES AND COSTS**

Petitioner's request for attorneys' fees and costs should also be denied. Under Public Officers Law § 89(4)(c), a court "may" award a petitioner who has "substantially prevailed" attorneys' fees and costs if (i) the agency had no reasonable basis for denying access; or (ii) the agency failed to respond to a request or appeal within the statutory time. If a petitioner does not substantially prevail, the inquiry is over and no fees are to be awarded. Even if statutory requirements are met, however, the decision to award attorneys' fees and costs remains within the court's discretion. *See Exoneration Initiative v. N.Y.C. Police Dep't.*, Index No. 104004, 2013 N.Y. Misc. LEXIS 4727 (Sup. Ct., N.Y. Co. Oct. 26, 2013), *aff'd in part and modified in part*, 11 N.Y.S.3d 139 (1st Dep't 2015).

As discussed in Points I and II *supra* and in Intervenors-Respondents' memoranda of law, Petitioner should not prevail in this action. It is thus axiomatic that Petitioner is not entitled to fees and costs. Even assuming *arguendo* that this Court grants Petitioner's motion to compel production of some or all of the redacted information, Petitioner should nevertheless be denied attorneys' fees and costs because DoITT had at least three reasonable grounds for denying access to the requested information. *See New York Times Co. v. NYPD*, 2011 N.Y. Misc. LEXIS 5182, at * 17 (Sup. Ct. N.Y. Co. Oct. 2, 2011) (rejecting claim for attorneys' fees where agency's reasons for denying access were not unreasonable), *aff'd in part, modified in part* 103 A.D.3d 405 (1st Dep't 2013). *Urban Justice Ctr. v. N.Y. Police Dep't.*, 2010 NY Slip Op 32400(U), ¶ 26, 2010 N.Y. Misc. LEXIS 4258 (Sup. Ct., N.Y. Co. Sep. 1, 2010) (denying petitioner's request for attorneys' fees because respondent had reasonable basis for denying access to the records at issue).

CONCLUSION

For the foregoing reasons and the reasons set forth in the papers submitted by the Intervenor-Respondents, DoITT respectfully requests that the Court deny the Verified Petition in its entirety and grant DoITT such other and further relief as the Court deems just and proper.

Dated: New York, NY
February 3, 2017

ZACHARY W. CARTER
Corporation Counsel of the
City of New York
Attorney for Respondent DoITT
100 Church Street
New York, NY 10007
Tel: (212) 356-0881
Fax: (212) 356-8760
ajacob@law.nyc.gov

By: 
Agnetha E. Jacob
Assistant Corporation Counsel