Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Special Access for Price Cap Local Exchange Carriers;	)	WC Docket No. 05-25
	)	
	)	
AT&T Corporation Petition for Rulemaking to Reform Regulation of Incumbent Local Exchange Carrier Rates for Interstate Special Access Services	)	RM-10593

ORDER AND DATA COLLECTION PROTECTIVE ORDER

Adopted: October 1, 2014 **Released: October 1, 2014**

By the Associate Chief, Wireline Competition Bureau:

I. INTRODUCTION

1. In this Order, the Wireline Competition Bureau (Bureau) adopts the attached Data Collection Protective Order (Protective Order) governing the process for designating, submitting, and accessing confidential and highly confidential information and data submitted in response to the Commission's special access data collection (Data Collection).[1] We also establish a Secure Data Enclave (SDE) to store data and information designated as Confidential Information, Highly Confidential Information and Highly Confidential Data, as those terms are defined in the Protective Order.[2] Authorized parties will be permitted to access the SDE at a physical location in the Washington, D.C. metropolitan area and remotely via a Virtual Private Network (VPN). Only those authorized persons who are Outside Counsel or Outside Consultants and not involved in Competitive Decision-Making, as those terms are defined in the Protective Order, can access the SDE.[3] The procedures we adopt in the

[1] *See Special Access for Price Cap Local Exchange Carriers; AT&T Corporation Petition for Rulemaking to Reform Regulation of Incumbent Local Exchange Carrier Rates for Interstate Special Access Services*, WC Docket No. 05-25, RM-10593, Report and Order and Further Notice of Proposed Rulemaking, 27 FCC Rcd 16318, 16340, para. 52 (2012) (*Data Collection Order* or *Data Collection FNPRM*); *Special Access for Price Cap Local Exchange Carriers; AT&T Corporation Petition for Rulemaking to Reform Regulation of Incumbent Local Exchange Carrier Rates for Interstate Special Access Services*, WC Docket No. 05-25, RM-10593, Report and Order, 28 FCC Rcd 13189 (Wireline Comp. Bur. 2013) *(Data Collection Implementation Order); Special Access for Price Cap Local Exchange Carriers; AT&T Corporation Petition for Rulemaking to Reform Regulation of Incumbent Local Exchange Carrier Rates for Interstate Special Access Services*, WC Docket No. 05-25, RM-10593, Order on Reconsideration, DA 14-1327 (Wireline Comp. Bur. rel. Sept. 15, 2014) (*Reconsideration Order*); App. A, Data Collection Protective Order, para. 1 (defining Data Collection).

[2] *See* App. A., Data Collection Protective Order, para. 1 (defining Confidential Information, Highly Confidential Information and Highly Confidential Data). We will provide additional details about the SDE and our procedures prior to making collected information available to authorized Reviewing Parties.

[3] See App. A., Data Collection Protective Order, para. 1 (defining Outside Counsel and Outside Consultants). Parties authorized to review Highly Confidential Information may also access Confidential and Highly Confidential Information (other than Highly Confidential Data described in Appendix B) outside the SDE. They may gain access to such information in electronic form by contacting the Bureau. Parties authorized to review only Confidential

(continued…)

Protective Order and the establishment of the SDE provide appropriate access to the public and allow them to participate meaningfully while protecting particularly competitively sensitive information from improper disclosure.

II. BACKGROUND

2. On December 11, 2012, the Commission adopted the *Data Collection Order* initiating a comprehensive data collection to assist the Commission in analyzing competition for special access services.[4] The Commission delegated authority to the Bureau to, among other things, amend the Data Collection based on public feedback, implement corrections to the Data Collection, and "take other such actions as are necessary to implement" the Data Collection.[5] The Bureau subsequently adopted the *Data Collection Implementation Order* clarifying the scope of the Data Collection, providing instructions for submitting information, and modifying and amending questions and definitions contained in the Data Collection.[6] On September 15, 2014, the Bureau adopted the *Reconsideration Order* amending the Data Collection to reflect the conditional approval received from the Office of Management and Budget (OMB) pursuant to the Paperwork Reduction Act (PRA) and announcing that responses to the Data Collection are due by December 15, 2014.[7]

3. Much of the data and information sought in the Data Collection are competitively sensitive and not publically available. For example, the Data Collection requires that certain providers and purchasers of special access and certain entities providing "best efforts" broadband Internet access service in areas where the incumbent local exchange carrier (ILEC) is subject to price cap regulation to submit data regarding locations with connections, prices charged to customers at the circuit-level, maps showing fiber routes and points of interconnection, revenues and expenditures.[8] Once the data are analyzed, the Commission plans to evaluate whether to change its existing special access regulatory framework, including its pricing flexibility rules, to better target regulatory relief where "actual and potential competition for special access is likely to constrain prices."[9]

4. The Freedom of Information Act (FOIA) requires the Commission to disclose reasonably described agency records requested by any person unless the records contain information falling within an exemption.[10] Under FOIA Exemption 4, which is most relevant to the instant Data Collection, the

(Continued from previous page)
Information are not permitted to access the SDE. However, they also may request Confidential Information in electronic form by contacting the Bureau. *See infra* para. 12; App. A, Data Collection Protective Order, para. 7.

[4] *See Data Collection Order*, 27 FCC Rcd 16318.

[5] *Id.* at 16340, para. 52.

[6] *Data Collection Implementation Order*, 28 FCC Rcd 13189.

[7] *See Reconsideration Order*, DA 14-1327, para. 1; *see also Data Collection Order*, 27 FCC Rcd at 16356, para. 94; *Commission Moves Forward with Special Access Data Collection*, WC Docket No. 05-25, RM-10593, Public Notice, DA 14-1201 (Wireline Comp. Bur. rel. Aug. 18, 2014); *see also* Notice of Office of Office of Management and Budget Action, OMB Control No. 3060-1197 (Aug. 15, 2014), *available at* http://www.reginfo.gov/public/do/PRAViewICR?ref_nbr=201311-3060-001# (last visited Aug. 27, 2014) (OMB approval of the Data Collection with change); *Special Access Proceeding; Effective Date for Data Collection*, 79 Fed. Reg. 57810 (Sept. 26, 2014) (announcing that the information collection requirement contained in the *Data Collection Order* is effective September 26, 2014).

[8] *See Data Collection Order*, 27 FCC Rcd at 16318.

[9] *See Special Access Data Collection FNPRM*, 27 FCC Rcd at 16346, para. 69; *Comment Deadlines Extended in Special Access Proceeding*, WC Docket No. 05-25, RM-10593, Public Notice, 28 FCC Rcd 11125 (Wireline Comp. Bur. 2013).

[10] *See* 5 U.S.C. § 552; *Examination of Current Policy Concerning the Treatment of Confidential Information Submitted to the Commission*, GC Docket 96-55, Report and Order, 13 FCC Rcd 24816, 24818 paras. 2-3 (1998) (*Policy Report and Order*).

government can withhold from public inspection "trade secrets and commercial or financial information obtained from a person and privileged or confidential."[11] The Commission's rules implementing FOIA and Exemption 4 list certain materials that are "not routinely available" for public inspection.[12] For materials not listed in the rules, parties can ask the Commission to withhold the material from public inspection on an *ad hoc* basis. The Commission can conditionally or unconditionally grant the request.[13] Consistent with this authority, the Commission has relied on protective orders to provide restricted access to information considered confidential.[14] A protective order can thus "serve the dual purpose of protecting competitively valuable information while still permitting limited disclosure for a specific public purpose."[15] By submitting information and documents stamped with appropriate confidentiality designations defined in a protective order, that submitting party is deemed to request that the information contained in the submission should be subject to protections under FOIA and the Commission's implementing rules.

5. The Bureau previously adopted protective orders in the special access proceeding. For example, the Bureau adopted a protective order covering the submission of proprietary or confidential information filed in the underlying rulemaking proceeding initiated in 2005.[16] A subsequent modification to this protective order and a second protective order were issued in connection with the Bureau's voluntary requests for information on the special access market.[17] The *Second Protective Order* created another level of protections for information deemed "Highly Confidential Information" – information that "if released to competitors would allow those competitors to gain a significant advantage in the marketplace."[18] Access to information designated as "Highly Confidential Information" under the *Second Protective Order* and its supplements is limited to parties that are insulated from the competitive decision-

[11] 5 U.S.C. § 552(b)(4). Even when an exemption applies, however, the Commission "is generally afforded the discretion to release the information on public interest grounds." *Policy Report and Order*, 13 FCC Rcd at 24818 para. 2.

[12] 47 C.F.R. § 0.457(d).

[13] 47 C.F.R. § 0.461(f)(4).

[14] *See, e.g., Rates for Interstate Inmate Calling Services*, WC Docket No. 12-375, Protective Order, DA 13-2434 (Wireline Comp. Bur. rel. Dec. 19, 2013); *Qwest Communications International Inc., Transferor, and CenturyTel, Inc. d/b/a CenturyLink, Transferee, Application for Transfer of Control Under Section 214 of the Communications Act*, WC Docket No. 10-110, Protective Order, 25 FCC Rcd 15238 (Wireline Comp. Bur. 2010).

[15] *Policy Report and Order*, 13 FCC Rcd at 24823, para. 9.

[16] *Special Access Rates for Price Cap Local Exchange Carriers*, WC Docket No. 05-25, Order, 20 FCC Rcd 10160, 10160, paras. 1-2 (Wireline Comp. Bur. 2005) *(First Protective Order*).

[17] *Special Access for Price Cap Local Exchange Carriers; AT&T Corporation Petition for Rulemaking to Reform Regulation of Incumbent Local Exchange Carrier Rates for Interstate Special Access Services*, WC Docket No. 05-25, RM-10593, Modified Protective Order, 25 FCC Rcd 15168 (Wireline Comp. Bur. 2010) (*Modified First Protective Order*); *Special Access for Price Cap Local Exchange Carriers; AT&T Corporation Petition for Rulemaking to Reform Regulation of Incumbent Local Exchange Carrier Rates for Interstate Special Access Services*, WC Docket No. 05-25, RM-10593, Second Protective Order, 25 FCC Rcd 17725, 17727-28, para. 6 (Wireline Comp. Bur. 2010) (*Second Protective Order*); Letter from Sharon E. Gillett, Chief, Wireline Competition Bureau, FCC, to Paul Margie, Wiltshire & Grannis LLP, WC Docket No. 05-25, RM-10593, 26 FCC Rcd 6571 (Wireline Comp. Bur. 2011) (granting a request for enhanced Confidential treatment for certain data pursuant to the *Second Protective Order*) (*First Supplement to Second Protective Order*); Letter from Sharon E. Gillett, Chief, Wireline Competition Bureau, FCC, to Donna Epps, Vice President, Federal Regulatory Affairs, Verizon, WC Docket No. 05-25, RM-10593, 27 FCC Rcd 1545 (Wireline Comp. Bur. 2012) (granting in part, denying in part, a request for Highly Confidential treatment pursuant to the *Second Protective Order*) (*Second Supplement to Second Protective Order*).

[18] *See Second Protective Order*, 25 FCC Rcd at 17727-28, para. 6; *First Supplement to Second Protective Order*, 26 FCC Rcd at 6571-72; *Second Supplement to Second Protective Order*, 27 FCC Rcd at 1545-49.

making activities of any entity in competition with or in a business relationship with the submitting party – outside counsel, their employees, and outside consultants retained to assist in the special access proceeding.[19]

6. Under the previously adopted protective orders, authorized persons request and obtain confidential information, including information designated as "Highly Confidential Information" under the *Second Protective Order* and its supplements, directly from the party submitting the information to the Commission. Persons seeking access to confidential information must first execute and file an acknowledgement of confidentiality with the Bureau, subject to the submitting party's objection.[20] Once authorized, the reviewing party is permitted to inspect confidential information," as appropriate, either at the offices of the submitting party's outside counsel or by receiving copies of the documents.[21]

7. The Data Collection presents unique challenges for parties submitting and seeking access to information to participate in the underlying rulemaking proceeding. Accordingly, we sought comment in a *Public Notice* on a new draft protective order to govern submission and review of confidential and highly confidential information and data submitted in response to the Data Collection.[22] AT&T, Inc. (AT&T) filed comments opposing our proposal as unnecessary given the earlier protective orders adopted in the proceeding.[23] CenturyLink, Inc. (CenturyLink) and Verizon and Verizon Wireless, Inc. (Verizon) generally supported our proposal but requested clarification and modification.[24] Cox Communications, Inc. (Cox) and the National Cable and Telecommunications Association (NCTA) implicitly supported a new protective order requesting heightened protections.[25]

III. DISCUSSION

A. Establishing a Secure Data Enclave and Adopting a New Protective Order

8. We find having a secure central database, an SDE, is necessary to allow parties to timely analyze the collected data and participate in the underlying rulemaking proceeding. Accordingly, we hereby establish an SDE and adopt the attached protective order that, among other things, sets forth the procedures for accessing data hosted at the SDE. The SDE will only contain data and information submitted in response to the Data Collection not data and information that was previously filed in this proceeding.[26] Prior protective orders will continue to govern the submission, review, and use of all other information and documents submitted in the underlying rulemaking proceeding.[27]

---

[19] *Second Protective Order*, 25 FCC Rcd at 17727-29, paras. 5, 12.

[20] *Modified First Protective Order*, 25 FCC Rcd at 15169-71, paras. 3, 7; *Second Protective Order*, 25 FCC Rcd at 17726-29, paras. 4, 12.

[21] *Modified First Protective Order*, 25 FCC Rcd at 15169-73, paras. 3, 20; *Second Protective Order*, 25 FCC Rcd at 17729-31, paras. 12, 20.

[22] *Wireline Competition Bureau Seeks Comment on Protective Order for Special Access Data Collection*, WC Docket No. 05-25, RM-10593, Public Notice, 28 FCC Rcd 9170, 9170 (Wireline Comp. Bur. 2013) (*Public Notice*).

[23] *See* AT&T Comments at 3-7.

[24] *See, e.g.* CenturyLink Comments at 1-3 (supporting the proposed protective order but asking the Commission to clarify the extent to which the Collection applies to non-public contracts or tariffs); Verizon Comments at 1-2 (supporting the proposed protective order but asking the Commission to clarify the definition of Highly Confidential Information and critiquing the distinction between Highly Confidential Information and Highly Confidential Data).

[25] *See* Cox Comments at 1-2; NCTA Comments at 1.

[26] The SDE will contain data and information that has been designated by a Submitting Party as Confidential Information, Highly Confidential Information or Highly Confidential Data, as those terms are defined in the Protective Order, as well as non-Confidential information.

[27] *Public Notice*, 28 FCC Rcd at 9170 n.5.

9. The scale and scope of the Data Collection dictates having a central repository for authorized parties to access and review information, and the prior protective orders do not accommodate in a practical way the use of a central repository. The estimated potential respondent universe for this Data Collection is 4,000 filers.[28] The Commission's analysis of the data will include, to the extent practicable, panel regressions and we expect Reviewing Parties will want to conduct similar econometric analyses to support their participation in the underlying rulemaking proceeding.[29] To conduct such analyses of all price cap areas nationwide, a Reviewing Party will need a complete data set. To obtain a complete data set under the prior protective orders, however, the authorized reviewer would have to request Highly Confidential Data from each Submitting Party directly. Such a process is neither feasible nor efficient when dealing with potentially thousands of respondents. A central repository is thus necessary for authorized parties to timely review and analyze the collected information and participate in the underlying rulemaking proceeding.

10. Moreover, having a central database containing information from every facilities-based provider of special access services in price cap areas nationwide justifies even greater measures to secure information from public disclosure than provided under prior protective orders. As Verizon correctly notes, some of the data collected "constitutes companies' most competitively sensitive business information" and includes "information on network maps and locations served that if disclosed could compromise network security."[30] We agree and therefore take steps above and beyond the restrictions contained in prior protective orders to secure this information, e.g., limitations on removing certain data from the SDE.

11. AT&T was the only party to oppose adoption of a new protective order arguing that the *Public Notice* did not identify any issues "unique" to the Data Collection that could not be addressed through the *Second Protective Order* and that a new protective order would establish a "cumbersome process."[31] We disagree with AT&T and, as explained above, find that the scale and scope of the Data Collection presents unique challenges unaddressed in prior protective orders necessitating our establishing the centralized SDE. We find that establishing an SDE coupled with the additional protections provided in the Protective Order balances the need of parties to participate in the rulemaking proceeding in a meaningful way with the competitively sensitive nature of the data collected. Accordingly, we hereby adopt the attached Protective Order and establish an SDE for analyzing data submitted in response to the Data Collection.

1. A Third-Party Vendor Will Host the SDE

12. The Commission has contracted with a third-party vendor to establish an SDE.[32] We evaluated hosting the SDE at the Commission for this one-time collection but find that an experienced third-party vendor with the necessary facilities already in place can host the SDE in a more cost-effective manner than could the Commission.[33] We will require the third-party vendor to provide both physical

[28] *See* Comprehensive Market Data Collection for Interstate Special Access Services, Supporting Statement, OMB Control No. 3060-1197, at 24 (rev. Aug. 2014), *available at* http://www.reginfo.gov/public/do/DownloadDocument?documentID=437246&version=2 (last visited Aug. 27, 2014).

[29] *Data Collection Implementation Order*, 28 FCC Rcd at 13192, para. 5.

[30] Verizon Comments at 2.

[31] *See* AT&T Comments at 3-7. AT&T acknowledged that there may be value in making data available via a central repository. *See* AT&T Comments at 5.

[32] The Commission has contracted with the National Opinion Research Center (NORC) at the University of Chicago, a non-profit "leader in the development and management of data in a protected environment," to host the SDE. *See* NORC at the University of Chicago, http://www.norc.org/Research/Capabilities/Pages/data-enclave.aspx (last visited Sept. 8, 2014).

[33] *See infra* paras. 14-22.

access at a single location in the Washington, D.C. metropolitan area and remote access to the SDE through a VPN using thin clients.[34]

13. Only those authorized persons who are Outside Counsel or Outside Consultants and not involved in Competitive Decision-Making, as those terms are defined in the Protective Order, can access the SDE. Upon request to the Bureau, a Reviewing Party may obtain copies of documents containing Confidential and Highly Confidential Information – but not copies of the Highly Confidential Data, as that term is defined in the Protective Order – outside the SDE subject to the applicable non-disclosure requirements.[35] When executing the Acknowledgement of Confidentiality, authorized parties may select a Confidential and Highly Confidential option, which requests access to the SDE and information and data contained therein, and a Confidential-only option which limits their access to Confidential Information, prohibiting access to Highly Confidential Data and Information as well as the SDE.[36]

14. An authorized Reviewing Party can access the SDE physical facility free of charge. The SDE vendor, however, can assess reasonable charges for remote access using a thin client. The thin clients will access the SDE through a VPN and will lack hard drives and the ability to save, email, download or print information from the SDE. Computer terminals within the SDE physical facility in the Washington, D.C. metropolitan area will have similar limitations. We will restrict the viewing of customer-identifiable information and the release of data from the SDE as discussed further in section II.A.3. The selected vendor has the appropriate security measures in place, including a robust tracking system as suggested by Cox, to monitor and protect against the unauthorized disclosure of competitively sensitive information.[37] As provided in the Protective Order, an authorized Reviewing Party may not improperly disclose Confidential and Highly Confidential Information, and the selected vendor is subject to similar non-disclosure requirements, and we will aggressively enforce these prohibitions.

15. We understand that some commenters find that restricting access to the data to a physical room would provide added protection against unauthorized disclosure[38] but agree with AT&T that limiting access to just a physical location would "increase each party's costs of participation, perhaps prohibitively," in the rulemaking proceeding.[39] Secure virtual data rooms are common in the private sector for accessing and reviewing sensitive information for transactions, mergers and litigation.[40] We are thus not adopting novel or untested security measures by taking advantage of such capabilities and can establish an SDE with the assistance of a third-party vendor that provides a secure yet convenient means for a Reviewing Party to analyze Confidential and Highly Confidential Data and Information submitted in response to the Data Collection.

---

[34] A thin client is a desktop or laptop computer, without a hard drive, which accesses applications and data remotely from a central server where all data processing and file storage are performed. *See Public Notice*, 28 FCC Rcd at 9172 n.10.

[35] *See* App. A, Data Collection Protective Order, para. 7.

[36] *See* App. C – Acknowledgement of Confidentiality. In lieu of accessing the SDE, authorized parties that have Confidential-only access may request from the Bureau electronic copies of documents containing Confidential Information as well as Redacted Highly Confidential Documents (which redact Highly Confidential Information). *See* App. A, Data Collection Protective Order, paras. 1 & 7.

[37] Cox Comments at 7-8.

[38] *See* Cox Comments at 6-7; NCTA Comments at 3; Verizon Comments at 2.

[39] *See* AT&T Comments at 5-7.

[40] *See, e.g.*, Merrill DataSite,® www.datasite.com (last visited Jan. 17, 2014) (providing an online virtual data room solution for sensitive business information for intellectual property litigation, mergers and acquisitions, etc.); Citrix ShareFile Virtual Data Room, www.sharefile.com/virtual-data-room/ (last visited Jan. 17, 2014); Firmex Virtual Data Rooms, www.firmex.com/virtual-data-rooms/ (last visited Jan. 17, 2014).

2. Analytical Tools Available in the SDE

16. In the *Public Notice*, the Bureau asked how software programs such as *SAS*® and *Stata*® could be made available (or installed) at a secure data environment for parties to analyze Highly Confidential Data.[41] AT&T commented that "[a]ccess to both of those programs, as well as any other software packages that parties indicate they would like to use, will be key to the parties' ability to properly analyze the data."[42] AT&T also asked the Commission to modify the proposed protective order to "permit the results of all analyses, as well as any computer programs or other methods of arriving at those analyses, to be stored on a mobile data storage medium."[43]

17. To help authorized parties review and evaluate the collected data, we will ensure that *SAS*® and *Stata*® are available in the SDE. We defer at this time to decide whether to provide additional software programs or to permit reviewing parties to bring additional software programs and or other outside information into the SDE. This decision depends on further discussions with the SDE vendor, the analytical tools the Reviewing Party seeks to utilize in the SDE, licensing costs, and the vendor's security concerns with a Reviewing Party bringing analytic tools into the SDE. We will address this issue prior to making the SDE available for access.

3. Restrictions on Reviewing and Removing Data and Analysis from the SDE

18. In the *Public Notice,* we sought comment on various methods of allowing restricted access to Highly Confidential Data in a secure environment.[44] Typically under protective orders, authorized parties are allowed to make and retain a limited number of copies of sensitive documents during the course of a proceeding. However, this Data Collection presents unique challenges given the scale, volume and competitively sensitive nature of the information collected. With the Data Collection containing detailed information on the facilities of every provider of special access in price cap areas nationwide, the risk of harm resulting from inadvertent disclosure is significantly greater than is typically the case in a Commission proceeding. We therefore find that additional restrictions on viewing certain information in the SDE and removing data from the SDE are justified.[45]

19. *Reviewing Data While in the SDE*. We asked for comment on whether to add "random noise" to the raw data or use other masking techniques to protect company-specific information while reviewing information within the SDE.[46] The sole commenter on this issue, AT&T, opposed these techniques because they may reduce the quality of their data analysis.[47] After considering the interests of Reviewing and Submitting Parties, we will allow authorized Reviewing Parties, i.e., Outside Counsel and Outside Consultants, to view raw Highly Confidential Data in the SDE absent any masking techniques with one exception. We will mask the names of customers reported by providers in their reported billing data with some other unique identifier. This limited use of masking will protect the customer's privacy interest while not adversely affecting analysis results.[48]

---

[41] *Public Notice*, 28 FCC Rcd at 9172 & n.11.

[42] AT&T Comments at 9.

[43] AT&T Comments at 8-9.

[44] *Public Notice*, 28 FCC Rcd at 9171.

[45] *See* CenturyLink Comments at 1-2; Cox Comments at 3, 4, 6; NCTA Comments at 2; Verizon Comments at 1-2.

[46] *Public Notice*, 28 FCC Rcd at 9172.

[47] *See* AT&T Comments at 10 (noting that the use of masking "techniques could adversely affect any analysis").

[48] *See, e.g.*, 47 C.F.R. § 64.2001 *et seq*. (Commission's rules protecting "customer proprietary network information" or CPNI); *see also FCC Enforcement Advisory: Telecommunications Carriers and Interconnected VoIP Providers Must File Annual Reports Certifying Compliance with Commission Rules Protecting Customer Proprietary Network Information*, EB Docket No. 06-36, Public Notice, 29 FCC Rcd 1102 (Enforcement Bur. 2014) (explaining that the (continued…)

20. *Removing Data from the SDE*. We will not allow Reviewing Parties to remove, e.g., download or print, Confidential Information, Highly Confidential Information and Highly Confidential Data from the SDE in order to prevent the inadvertent disclosure of information and data on a large scale. Reviewing Parties may request from the Bureau copies of Confidential and Highly Confidential Information, as appropriate, except for information defined as Highly Confidential Data.[49] That said, we acknowledge that interested parties may want to reference specific data in their comments filed in the underlying special access proceeding. We clarify that authorized parties are allowed to reference specific data points in their comments, subject to designation and redaction requirements as outlined in the Protective Order. The availability of remote access greatly diminishes the need to remove information from the SDE as authorized parties can instead access the SDE as easily as accessing information on their own internal network or local hard drive. In addition, we will provide each authorized Reviewing Party with a virtual locker on the SDE for saving information, notes and analysis results. Only the authorized Reviewing Party will have access to its designated virtual locker. We again note that the vendor will have in place a robust tracking system that will record all information accessed by the user while in the SDE to ensure compliance with the restrictions contained in the Protective Order. Accordingly, this restriction provides added protection against inadvertent disclosure while not unduly hindering a party's ability to meaningfully participate in the rulemaking proceeding.

21. We will allow an authorized Reviewing Party to remove their analysis results from the SDE. We examined whether to require that data research results conform to one or more standard rules for identifying disclosure risk before permitting those results to leave the SDE and whether aggregation rules are sufficient to protect commercially sensitive data.[50] AT&T opposed standard rules for identifying disclosure risk before permitting results to leave the SDE, raising feasibility and attorney work product concerns.[51] We agree and will not review and release results subject to disclosure standards. The SDE vendor will, however, process requests for the release of results to ensure that the release will not include data sets. In addition, the SDE vendor will track and save a copy of the analysis results removed from the SDE but will not share this information with the Commission. We emphasize that these results maintain their identity as Confidential Information, Highly Confidential Information, and/or Highly Confidential Data as those terms are defined in the Protective Order, and may not be disclosed except as provided by that order.

4. Submitting Data and the Authorization Process for Accessing Data and Information

22. *Submission Process*. In the *Public Notice*, we sought comment on our proposal for the electronic submission of Confidential and Highly Confidential Information and Highly Confidential Data.[52] Specifically, we proposed having a secure web portal ("Special Access Web Portal") through which parties would submit their responses to those Data Collection questions that require narrative responses and any supporting documentation.[53] In addition, for larger files (up to eleven gigabytes in size), we proposed having parties electronically deliver to the Commission a database container using an

(Continued from previous page)
Commission's CPNI rules provide important consumer privacy protections regarding sensitive information carriers have about their customers by virtue of their business relationship).

[49] *See supra* para. 13; App. A, Data Collection Protective Order, para. 7.

[50] *Public Notice*, 28 FCC Rcd at 9172.

[51] AT&T Comments at 9-10.

[52] *Public Notice*, 28 FCC Rcd at 9171.

[53] *See Reconsideration Order*, DA 14-1327, App. A – Mandatory Data Collection, Question II.A.12(b) (requiring name and unique numerical identifier for each customer); Question II.A.12(c) (requiring the customer's location); Question II.A.12(e) (requiring type of circuit and bandwidth); Question II. A.12(g) (requiring number of units billed for each circuit element).

SSH File Transfer Protocol (SFTP) and proposed manual submission on storage devices for even larger files.[54] We did not receive any comments on this proposal. After further internal technical discussions, we have decided to use the Special Access Web Portal as the primary mechanism for respondents to deliver their data and information to the Commission. Respondents can make arrangements with Commission staff to deliver larger files that exceed the technical limitations of the Special Access Web Portal using a portable electronic storage medium.[55] We also proposed that parties also submit redacted versions of Confidential and Highly Confidential submissions through the Commission's Electronic Comment Filing System (ECFS).[56] We did not receive any comments on this proposal and will proceed as we proposed. However, Submitting Parties do not need to submit via ECFS redacted versions of documents or data containers containing Highly Confidential Data submitted to the Special Access Web Portal.

23. *Authorization Process*. We did not receive any comments regarding our proposed authorization process for accessing Confidential and Highly Confidential Information. Accordingly, we will proceed as proposed. That is, only parties signing the Acknowledgement of Confidentiality (Acknowledgement) attached to the Protective Order will have access to Confidential Information, Highly Confidential Information, and Highly Confidential Data submitted in response to the Data Collection, as appropriate. Access to Highly Confidential Information and Highly Confidential Data is limited to Outside Counsel and Outside Consultants and their employees who are not involved in the Competitive Decision-Making activities of a competitor of a Submitting Party or a person with whom the Submitting Party does business. A Submitting Party will have the opportunity to object to persons or entities seeking to review their Confidential Information, Highly Confidential Information, and Highly Confidential Data. Specifically, as described in the Protective Order, we will periodically release a public notice identifying those parties that have filed a signed Acknowledgement with the Commission and requested access to Confidential Information, Highly Confidential Information, and Highly Confidential Data.[57] A Submitting Party will have at least five business days to object to the access sought by a requesting party.[58] Absent the filing of an objection, the requesting party will have access to Confidential Information, Highly Confidential Information, and Highly Confidential Data as set forth in the Protective Order. We will announce when the Commission is ready to receive executed Acknowledgements of Confidentiality.[59]

---

[54] *Public Notice*, 28 FCC Rcd at 9171. Since the release of the *Public Notice*, we have provided instructions for the Collection that include data format specifications for the relevant questions. *See Reconsideration Order*, DA 14-1327, App. B – Instructions for Data Collection for Special Access Proceeding; *see also Data Collection Implementation Order*, 28 FCC Rcd at 13219-13300, App. A. Respondents will fill their database containers in accordance with these specifications, and we will provide validation to ensure the data meets the requisite specifications prior to delivery.

[55] The Bureau will separately announce when the Special Access Web Portal is operational. For narrative responses and data containers submitted in response to the Data Collection, the maximum file size accepted by the Special Access Web Portal is 2 gigabytes. Further, data containers submitted in response to the Data Collection will need to be submitted in a compressed ".zip" file through the Special Access Web Portal.

[56] *Public Notice*, 28 FCC Rcd at 9171 & n. 8 (*citing Applications of Comcast Corp., General Elec. Co., and NBC Universal, Inc. for Consent to Assign or Transfer Control of Licenses or Authorizations*, Protective Order, 26 FCC Rcd 2045 (Media Bur. 2011); *Applications of AT&T Inc. and Deutsche Telekom AG for Consent to Assign or Transfer Control of Licenses and Authorizations*, Second Protective Order (Revised), 26 FCC Rcd 8801 (Wireless Telecom. Bur. 2011), *modified*, 26 FCC Rcd 10288 (Wireless Telecom. Bur. 2011)).

[57] *See* App. A, Data Collection Protective Order, para. 5. In addition to identifying the requesting party, we will include details about the requesting party, *e.g.*, job title, employer, client represented, intended purpose for accessing data, to help Submitting Parties evaluate whether to object to the access sought.

[58] *See* App. A, Data Collection Protective Order, at para. 5.

[59] This announcement will occur in connection with the announcement that the SDE is available for access.

24. In addition, we sought comment in the *Public Notice* on whether to continue to require support staff that do not substantively examine Confidential Information to sign and file a separate Acknowledgement.[60] We did not receive any comments addressing this issue. Accordingly, we will not require support staff employed by Outside Counsel and Outside Consultants who do not substantively examine Confidential Information, Highly Confidential Information or Highly Confidential Data to execute separate Acknowledgements.[61] However, we do require paralegals, analysts and other employees of the Reviewing Party who substantively examine Confidential Information, Highly Confidential Information or Highly Confidential Data to execute the Acknowledgement. We rely on the obligations that the Protective Order imposes on Outside Counsel and Outside Consultants, who employ such support staff, to comply with the Protective Order, to ensure that there is no unauthorized disclosure of Confidential Information, Highly Confidential Information or Highly Confidential Data by either themselves or any of their employees, and to ensure that there are adequate procedures in place at their firm or workplace to prevent any such unauthorized disclosure. This change will reduce the administrative burden on parties seeking access to data.

B. Revisions to Categories of Highly Confidential Information and Data

25. The Protective Order divides submitted documents, data and information into four categories: (1) documents and information that are presumptively Highly Confidential Information; (2) documents, data containers and data that are presumptively Highly Confidential Data; (3) documents and information designated by the filing parties as Confidential Information; and (4) documents and information that are not Confidential and will be made available to the general public. In Appendix A to the proposed protective order, we identified those types of data and information that we proposed to treat as Highly Confidential Information and Highly Confidential Data.[62] We sought comment on these designations.

26. Cox urges the Bureau to broaden the categories of data and information that may be designated for Highly Confidential treatment.[63] Specifically, Cox states that the following categories of information sought in the Data Collection should be considered Highly Confidential as it would, if released, provide competitors and customers with detailed information with which they could use to "gain valuable negotiating leverage" with Cox and its competitors:[64]

- The business justification for the *Term* or *Volume Commitments* associated with any *Tariff* or agreement offered for the sale of *Dedicated Services*.[65]

[60] *Public Notice*, 28 FCC Rcd at 9172.

[61] For example, an administrative assistant of an Outside Counsel of Record would not be required to execute a separate Acknowledgement if they perform administrative tasks only, not substantive analysis, for the Outside Counsel of Record.

[62] *See* App. A, Data Collection Protective Order.

[63] Cox Comments at 3-4.

[64] Cox Comments at 4-5.

[65] *See* Cox Comments at 3. The information in which Cox seeks Highly Confidential treatment is captured in Question II.A.19 of the Collection, which is directed at *Competitive Providers*. *Reconsideration Order*, DA 14-1327, App. A, Question II.A.19. Similarly, Question II.B.12(r) of the Collection, which is directed at *ILECs*, captures the business justification for the *Term* or *Volume Commitments* associated with *Tariff Plans* and *Contract-Based Tariffs* offered for the purchase of *DS1*, *DS3*, and/or *PBDS* services (which are included in the scope of *Dedicated Services*). *See id.* App. A, Question II.B.12(r).

- Detailed information on the length of time it takes to complete the process of connecting *End User Channel Terminations* to a new *Transport Provider*, including limitations on the number of circuits that can be moved within a given period of time.[66]
- Information on how connecting to a new *Transport Provider* impacts the company's prices, including the rates that apply before and after the requested change.[67]
- Detailed information on the terms and conditions of contracts by which a company obtains special access services for its own use or as an input to its retail services.[68]
- Information on whether a company either offers to negotiate time lines on a case-by-case basis or whether vendors offer it such negotiating opportunities including details regarding how long it took for an *ILEC* or *Competitive Provider* to connect your *End-user Channel Terminations* to another *Transport Provider* and whether you had an opportunity to negotiate time lines on a case-by-case basis.[69]
- Information on the purchase of circuits under a volume commitment, including the provider, the precise nature of the volume commitment, and a description of the specific terms and conditions under the applicable tariff sections.[70]

27. Only those categories of information specifically described in Appendix B to the Protective Order are presumptively entitled to Highly Confidential treatment with respect to the Data Collection in the special access proceeding. We agree with Cox, however, that for some questions the categories of information referenced above could include information that is among a company's most competitively sensitive business information.[71] Accordingly, we revise Appendix B to the Protective Order to the extent that these categories of information collected contain Highly Confidential Information or Highly Confidential Data.[72] We have also updated the categories in Appendix B to reflect changes to

[66] *See* Cox Comments at 3. This information is captured in Questions II.E.10(b)-(c) and II.F.9(b)-(c) of the Collection. *See Reconsideration Order*, DA 14-1327, App. A, Questions II.E.10(b)-(c), II.F.9(b)-(c).

[67] *See* Cox Comments at 3. This information is captured in Questions II.E.10(d)-(e) and II.F.9(d)-(e) of the Collection. *See Reconsideration Order*, DA 14-1327, App. A, Questions II.E.10(d)-(e), II.F.9(d)-(e).

[68] *See* Cox Comments at 4. This information is captured by Questions II.E.9 and II.F.8 of the Collection. *See Reconsideration Order*, DA 14-1327, App. A, Questions II.E.9, II.F.8; *see also*, CenturyLink Comments at 2-3 (seeking clarification of the extent to which Question II.F.8 seeks Highly Confidential non-tariffed agreements versus publically available tariffed agreements).

[69] *See* Cox Comments at 4. This information is captured in Questions II.E.10(b)-(c) and II.F.9(b)-(c) of the Collection. *See Reconsideration Order*, DA 14-1327, App. A, Questions II.E.10(b)-(c), II.F.9(b)-(c).

[70] *See* Cox Comments at 4. The information Cox seeks Highly Confidential treatment is now captured in Questions II.E.11(a)-(g) and II.F.10(a)-(g) of the Collection. *See Reconsideration Order*, DA 14-1327, App. A, Questions II.E.11(a)-(g), II.F.10(a)-(g). Cox requested Highly Confidential treatment for Tariff and section numbers of the specific terms and conditions, Cox Comments at 4, information which is captured by Questions II.E.11(c) and II.F.10(c) of the Collection. *See Reconsideration Order*, DA 14-1327, App. A, Question II.E.11(c), II.F.10(c). We find that the Tariff and section numbers captured in Questions II.E.11(c) and II.F.10(c) of the Collection do not rise to the level of competitively sensitive information to warrant Highly Confidential treatment. That said, submitting parties may request Confidential treatment for this information consistent with the Protective Order.

[71] *See* Cox Comments at 4-5.

[72] *See* App. A, Data Collection Protective Order, paras. 1-2; *id*., App. B ("Data and Information Eligible for Highly Confidential Treatment"). To the extent that portions of the documents submitted do not contain Highly Confidential Information (*e.g.*, information that is already publicly available such as information available in a publicly-filed tariff), may be produced in unredacted format or submitted as Confidential pursuant to the Protective Order.

the revised Data Collection questions in light of the *Data Collection Implementation Order* and the *Reconsideration Order*.[73]

C. Record Retention and Disposal After the Proceeding is Terminated

28. As set forth in the Protective Order, a Reviewing Party must destroy or return to the Submitting Party any Confidential Information, Highly Confidential Information and/or Highly Confidential Data received within two weeks after conclusion of the special access proceeding and any administrative or judicial review. Cox requests that the Commission also "either return or destroy confidential information in its possession once the proceeding has terminated."[74] We are unable to grant Cox's request. We will maintain and dispose of information obtained in the Data Collection in accordance with the applicable statutory requirements. Records of the Commission, like any U.S. Government agency, may not be destroyed except pursuant to Title 44, Chapter 33 of the U.S. Code.[75] Pursuant to that provision, the Commission is required submit to the National Archives and Records Administration (NARA) lists and schedules of records in the Commission's custody, which, among other things, includes schedules proposing the disposal of records that do not have sufficient value to warrant preservation.[76] NARA determines whether an agency may dispose of agency records.[77] Accordingly, we will maintain and dispose of information filed in response to the Data Collection consistent with the NARA-imposed schedules.[78]

IV. CONCLUSION

29. We conclude that the Protective Order strikes an appropriate balance by protecting competitively sensitive information while still allowing interested parties to review the data collected and participate in the underlying rulemaking proceeding. Accordingly, we adopt the attached Protective Order. We stress that the Protective Order governs submissions related to the Data Collection and does not supersede or modify protective orders previously issued in the special access proceeding.[79] The prior protective orders remain in effect and govern access to other documents submitted in the proceeding.[80]

[73] *See Data Collection Implementation Order*, 28 FCC Rcd at 13302-32, App. B; *Reconsideration Order*, DA 14-1327, App. A.

[74] Cox Comments at 8.

[75] *See* 44 U.S.C. §§ 3301, *et seq*. (disposal of records); 44 U.S.C. § 3314 (Title 44, Chapter 33 provides the exclusive procedures for disposing of U.S. Government Records).

[76] 44 U.S.C. § 3033.

[77] 44 U.S.C. § 3033a.

[78] *See* App. A, Data Collection Protective Order, para. 18.

[79] *See Data Collection Order*, 27 FCC Rcd 16318.

[80] *See Modified First Protective Order*, 25 FCC Rcd 15168; *Second Protective Order*, 25 FCC Rcd 17725; *First Supplement to Second Protective Order*, 26 FCC Rcd 6571; *Second Supplement to Second Protective O*rder, 27 FCC Rcd 1545.

V. ORDERING CLAUSE

30. *Authority.* This Protective Order is issued pursuant to sections 4(i), 5, 201-205, 211, 215, 218, 219, 303(r), and 332 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 154(i), 155, 201-205, 211, 215, 218, 219, 303(r), and 332, Section 4 of the Freedom of Information Act, 5 U.S.C. § 552(b)(4), and authority delegated under section 0.291 of the Commission's rules, 47 C.F.R. § 0.291, and the authority delegated by the Commission in the *Data Collection Order*, 27 FCC Rcd 16318, 16340, para. 52 (2012), and is effective upon its adoption.

FEDERAL COMMUNICATIONS COMMISSION

Deena M. Shetler
Associate Chief
Wireline Competition Bureau

APPENDIX A

Data Collection Protective Order

WC Docket No. 05-25
RM-10593

1. *Definitions*. As used herein, capitalized terms not otherwise defined in this Data Collection Protective Order shall have the following meanings:

"Acknowledgment" means the Acknowledgment of Confidentiality attached as Appendix C.

"Competitive Decision-Making" means a person's activities, association, or relationship with any of his or her clients involving advice about or participation in the relevant business decisions or the analysis underlying the relevant business decisions of the client in competition with or in a business relationship with the Submitting Party.

"Confidential Information" means information that is not otherwise available from publicly available sources and that is subject to protection under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, and the Commission's implementing rules.

"Counsel" means In-House Counsel and Outside Counsel of Record.

"Data Collection" or "Special Access Data Collection" means the data collection established in *Special Access for Price Cap Local Exchange Carriers; AT&T Corporation Petition for Rulemaking to Reform Regulation of Incumbent Local Exchange Carrier Rates for Interstate Special Access Services*, WC Docket No. 05-25, RM-10593, Report and Order and Further Notice of Proposed Rulemaking, 27 FCC Rcd 16318 (2012) (*Data Collection Order*), including the submission of Stamped Confidential and Highly Confidential Documents, Confidential and Highly Confidential Information, and Highly Confidential Data.

"Document" means any written, recorded, electronically stored, or graphic material, whether produced or created by the Submitting Party or another person. For the sake of clarity, the term "document" includes responses created and submitted to the Commission electronically.

"Highly Confidential Data" means information that meets the definition of Highly Confidential Information and is described as Highly Confidential Data in Appendix B to this Data Collection Protective Order, as the same may be amended from time to time.

"Highly Confidential Information" means information that is not otherwise available from publicly available sources; that the Submitting Party has kept strictly confidential; that is subject to protection under FOIA and the Commission's implementing rules; that the Submitting Party claims constitutes some of its most sensitive business data which, if released to competitors or those with whom the Submitting Party does business, would allow those persons to gain a significant advantage in the marketplace or in negotiations; and that is described in Appendix B to this Data Collection Protective Order, as the same may be amended from time to time.

"In-House Counsel" means an attorney employed by a Participant in this proceeding or employed by an affiliated entity and who is actively engaged in the conduct of this proceeding, provided that such attorney is not involved in Competitive Decision-Making. (In this regard, an In-House Counsel's employer is considered his or her client.)

"Outside Counsel of Record" or "Outside Counsel" means the attorney(s), firm(s) of attorneys, or sole practitioner(s), as the case may be, retained by a Participant in this proceeding, provided that such attorneys are not involved in Competitive Decision-Making. The term "Outside Counsel of Record" includes any attorney representing a non-commercial Participant in this proceeding, provided that such attorney is not involved in Competitive Decision-Making.

"Outside Consultant" means a consultant or expert retained for the purpose of assisting Outside Counsel or a Participant in this proceeding, provided that such consultant or expert is not involved in Competitive Decision-Making. The term "Outside Consultant" includes any consultant or expert employed by a non-commercial Participant in this proceeding, provided that such consultant or expert is not involved in Competitive Decision-Making.

"Outside Firm" means a firm, whether organized as a partnership, limited partnership, limited liability partnership, limited liability company, corporation or otherwise, of Outside Counsel or Outside Consultants.

"Participant" means a person or entity that has filed, or has a good faith intention to file, material comments in this proceeding.

"Redacted Confidential Document" means a copy of a Stamped Confidential Document where the Confidential Information has been redacted.

"Redacted Highly Confidential Document" means a copy of a Stamped Highly Confidential Document where the Highly Confidential Information has been redacted.

"Reviewing Party" means a person or entity who has obtained access to Confidential or Highly Confidential Information (including Stamped Confidential Documents and Stamped Highly Confidential Documents) pursuant to paragraphs 5 or 9 of this Data Collection Protective Order.

"Secure Data Enclave" or "SDE" means a secure environment, as established by the Commission, where Reviewing Parties may view Highly Confidential Data.

"Special Access Web Portal" means the secure website interface, established by the Commission, through which a Submitting Party submits its responses to the Data Collection which shall constitute a filing with the Secretary's Office. Further information on accessing the Special Access Web Portal will be announced in a Public Notice.

"Stamped Confidential Document" means any document, or any part thereof, that contains Confidential Information and that bears the legend (or which otherwise shall have had the legend recorded upon it in a way that brings its attention to a reasonable examiner) "CONFIDENTIAL INFORMATION – SUBJECT TO PROTECTIVE ORDERS IN WC DOCKET NO. 05-25 BEFORE THE FEDERAL COMMUNICATIONS COMMISSION," unless the Commission determines, *sua sponte* or by request pursuant to sections 0.459 or 0.461 of its rules,[1] that any such document is not entitled to confidential treatment. By designating a document a "Stamped Confidential Document," a Submitting Party signifies and represents that it contains Confidential Information.

"Stamped Highly Confidential Document" means any document, or any part thereof, that contains Highly Confidential Information and that bears the legend (or which otherwise shall have had the legend recorded upon it in a way that brings its attention to a reasonable examiner) "HIGHLY CONFIDENTIAL INFORMATION – SUBJECT TO PROTECTIVE ORDERS IN WC DOCKET NO. 05-25 BEFORE THE FEDERAL COMMUNICATIONS COMMISSION," unless the Commission determines, *sua sponte* or by request pursuant to sections 0.459 or 0.461 of its rules, that any such document is not entitled to highly confidential treatment. By designating a document a "Stamped Highly Confidential Document," a Submitting Party signifies and represents that it contains Highly Confidential Information.

"Submitting Party" means a person or entity who submits Confidential or Highly Confidential Information.

2. *Effect of Designation*. By designating documents, data and information as Confidential or Highly Confidential under this Data Collection Protective Order, a Submitting Party will be deemed to

[1] 47 C.F.R. §§ 0.459, 0.461.

have submitted a request that the material not be made routinely available for public inspection under the Commission's rules.[2] Any person wishing to challenge the designation of a document, portion of a document or information as Confidential or Highly Confidential must file such a challenge at the Commission and serve it on the Submitting Party. The Submitting Party must file any reply within five business days, and include a justification for treating the information as Confidential or Highly Confidential, as appropriate.[3] The documents and information challenged will continue to be accorded Confidential or Highly Confidential treatment until the Commission acts on the request and all subsequent appeal and stay proceedings have been exhausted.[4] Any decision on whether the materials should be accorded Confidential or Highly Confidential treatment does not constitute a resolution of the merits concerning whether such information would be released publicly by the Commission upon a proper request under our rules implementing FOIA.[5]

3. *Submission of Stamped Confidential, Stamped Highly Confidential Documents, and data containers containing Highly Confidential Data*. For Documents submitted in response to the Data Collection, a Submitting Party shall submit to the Secretary's Office via the Special Access Web Portal one copy of each Stamped Confidential Document, each Stamped Highly Confidential Document, and the data container containing Highly Confidential Data it seeks to file with the Commission. Except with regard to the data container containing Highly Confidential Data, each page of the Stamped Confidential Document or Stamped Highly Confidential Document shall be stamped "CONFIDENTIAL INFORMATION – SUBJECT TO PROTECTIVE ORDERS IN WC DOCKET NO. 05-25 BEFORE THE FEDERAL COMMUNICATIONS COMMISSION" or "HIGHLY CONFIDENTIAL INFORMATION – SUBJECT TO PROTECTIVE ORDERS IN WC DOCKET NO. 05-25 BEFORE THE FEDERAL COMMUNICATIONS COMMISSION," as appropriate. Data containers submitted to the Commission in response to the Data Collection through the Special Access Web Portal are presumed to contain Highly Confidential Data described in Appendix B and will be treated accordingly. A Submitting Party can make arrangements with Commission staff to deliver files such as data containers that exceed the technical limitations of the Special Access Web Portal using a portable electronic storage medium which likewise is presumed to contain Highly Confidential Data described in Appendix B and will be treated accordingly. In addition, with respect to each Stamped Confidential Document or Stamped Highly Confidential Document submitted, each Submitting Party shall also file through the Commission's Electronic Comment Filing System ("ECFS") in WC Docket No. 05-25and RM-10593 a copy of the respective Redacted Confidential or Redacted Highly Confidential Document and an accompanying cover letter which shall reference WC Docket No. 05-25 and RM-10593.[6] Each Redacted Confidential or Redacted Highly Confidential Document shall have the same pagination as the Stamped Confidential or Highly Confidential Document from which it is derived. Each page of the Redacted Confidential Document or Redacted Highly Confidential Document and the accompanying cover letter shall be stamped "REDACTED – FOR PUBLIC INSPECTION." To the extent that any page of the filing contains both Confidential or Highly Confidential Information and non-confidential information, only the Confidential Information and Highly Confidential Information may be redacted and the page of the unredacted filing shall clearly distinguish among the Confidential Information, the Highly Confidential Information, and the non-confidential information.

[2] *See* 47 C.F.R. §§ 0.459(a), 0.459(a)(3).

[3] *See* 47 C.F.R. § 0.459(b).

[4] *See* 47 C.F.R. § 0.459(g).

[5] *See* 47 C.F.R. §§ 0.459(h), 0.461.

[6] If a party is not able to submit a copy of the Redacted Confidential Document or Redacted Highly Confidential Document via ECFS, it must file two copies of the Redacted Confidential Document or Redacted Highly Confidential Document with the Secretary's Office along with the appropriately stamped cover letter.

4. *Copying Sensitive Documents*. If, in the reasonable judgment of the Submitting Party, a Stamped Highly Confidential Document contains information so sensitive that copying of it should be restricted, the Submitting Party may mark the document with the legend "Additional Copying Restricted." Each Outside Firm shall receive only one copy of the document and no more than two additional copies, in any form, shall be made. Application for relief from this restriction against further copying may be made to the Commission, with notice to Counsel of Record for the Submitting Party, which will be granted only for cause.

5. *Procedure for Obtaining Access to Confidential Information and Highly Confidential Information*. Access to Highly Confidential Information (including Stamped Highly Confidential Documents) is limited to Outside Counsel of Record, Outside Consultants, and those employees of Outside Counsel and Outside Consultants described in paragraph 9. Any person seeking access to Confidential Information or Highly Confidential Information subject to this Data Collection Protective Order shall sign and date the Acknowledgment agreeing to be bound by the terms and conditions of this Data Collection Protective Order; file the Acknowledgment with the Wireline Competition Bureau ("Bureau"), on behalf of the Commission, and send a copy to SpecialAccess@fcc.gov. The Acknowledgment does not need to be served on the Submitting Parties. The Bureau periodically will issue a Public Notice identifying all people who have filed Acknowledgments (the "Acknowledgment Public Notice") as the Acknowledgments are received. Each Submitting Party shall have an opportunity to object to the disclosure of its Stamped Confidential Documents, Stamped Highly Confidential Documents, Confidential Information, and Highly Confidential Information to any person filing an Acknowledgment. A Submitting Party must file any such objection at the Commission and serve it on Counsel representing, retaining, or employing such person within the time period specified in the Acknowledgment Public Notice, generally five business days. Except for persons described in paragraph 9, persons filing Acknowledgments shall not have access to Stamped Confidential Documents, Stamped Highly Confidential Documents, Confidential Information, or Highly Confidential Information before the period for filing objections has passed; persons described in paragraph 9 shall have access to Stamped Confidential Documents, Stamped Highly Confidential Documents, Confidential Information, and Highly Confidential Information upon the filing of their Acknowledgment, except that such access shall be prohibited if an objection is filed. If a Submitting Party files additional Stamped Confidential Documents, Stamped Highly Confidential Documents, Confidential Information, or Highly Confidential Information, it must file any objection to the disclosure of those additional documents and information to any Reviewing Party before or contemporaneous with filing the additional documents or information. Until any objection is resolved by the Commission and, if appropriate, by any court of competent jurisdiction, and unless such objection is resolved in favor of the person seeking access, a person subject to an objection from a Submitting Party shall not have access to relevant Stamped Confidential Documents, Stamped Highly Confidential Documents, Confidential Information, or Highly Confidential Information.

6. *Review of Highly Confidential Data.* A Reviewing Party may inspect and analyze Highly Confidential Data only at the Secure Data Enclave (SDE), either at its physical location in the Washington, D.C. metropolitan area or by accessing the SDE remotely through a Virtual Private Network (VPN) using a thin client. A Reviewing Party may not download, print out or otherwise remove any Highly Confidential Data from the SDE (however accessed). A Reviewing Party may store its analyses in a virtual locker located in the SDE and accessible only to that party. A Reviewing Party may obtain physical or electronic copies of its analyses from the SDE administrator upon request, and at cost; the SDE administrator will ensure that the copies contain only the analyses and not any underlying raw data.

7. *Review of Stamped Confidential Documents and Stamped Highly Confidential Documents.* A Reviewing Party may request, as appropriate, a complete set of Stamped Confidential Documents and a complete set of Stamped Highly Confidential Documents (other than Highly Confidential Data) in electronic form by contacting the Bureau. All copies of documents received must be returned or destroyed in accordance with the terms of paragraph 18. A Reviewing Party may inspect

Stamped Confidential Documents, Stamped Highly Confidential Documents and Highly Confidential Data at the Secure Data Enclave.

8. *Use of Confidential and Highly Confidential Information*. Persons obtaining access to Confidential and Highly Confidential Information (including Stamped Confidential Documents, Stamped Highly Confidential Documents, and Highly Confidential Data) under this Data Collection Protective Order shall use the information solely for the preparation and conduct of this proceeding before the Commission and any subsequent judicial proceeding arising directly from this proceeding and, except as provided herein, shall not use such documents or information for any other purpose, including without limitation business, governmental, or commercial purposes, or in any other administrative, regulatory or judicial proceedings. Should the Commission rely upon or otherwise make reference to any Confidential or Highly Confidential Information in its decision in this proceeding, it will do so by redacting any Confidential or Highly Confidential Information from the public version of the decision and by making the unredacted version of the decision available only to a court and to those persons entitled to access to Confidential or Highly Confidential Information under this Data Collection Protective Order, as appropriate.

9. *Permissible Disclosure*. A Reviewing Party may discuss and share the contents of Stamped Confidential Documents, Stamped Highly Confidential Documents, Confidential Information, and Highly Confidential Information with another Reviewing Party, as appropriate, and with the Commission and its staff. A Submitting Party's Stamped Confidential Documents, Stamped Highly Confidential Documents, Confidential Information, and Highly Confidential Information may also be disclosed to employees and Counsel of the Submitting Party. Subject to the requirements of paragraph 5, a Reviewing Party may disclose Stamped Confidential Documents, Stamped Highly Confidential Documents, Confidential Information, and Highly Confidential Information to: (1) paralegals or other employees of such Reviewing Party assisting them in this proceeding; and (2) employees of third-party contractors involved solely in one or more aspects of organizing, filing, coding, converting, storing, or retrieving documents or data or designing programs for handling data connected with this proceeding, or performing other clerical or ministerial functions with regard to documents connected with this proceeding.

10. *Filings with the Commission*. Parties filing comments or other filings in the special access rulemaking proceeding, WC Docket No. 05-25, that contain Confidential Information or Highly Confidential Information derived from the data submitted in response to the Data Collection shall submit to the Secretary's Office one copy of the filing containing the Confidential or Highly Confidential Information (the "Confidential Filing") and an accompanying cover letter. The cover or first page of the Confidential Filing and each page of the Confidential Filing that contains or discloses only Confidential Information shall be clearly marked "CONFIDENTIAL INFORMATION – SUBJECT TO PROTECTIVE ORDERS IN WC DOCKET NO. 05-25 BEFORE THE FEDERAL COMMUNICATIONS COMMISSION." The cover or first page of the Confidential Filing and each page of the Confidential Filing that contains or discloses Highly Confidential Information shall be clearly marked "HIGHLY CONFIDENTIAL INFORMATION – SUBJECT TO PROTECTIVE ORDERS IN WC DOCKET NO. 05-25 BEFORE THE FEDERAL COMMUNICATIONS COMMISSION." The accompanying cover letter shall also contain the appropriate legend. The Confidential Filing shall be made under seal, and will not be placed in the Commission's public file. The party shall submit a copy of the filing in redacted form, *i.e.*, containing no Confidential or Highly Confidential Information (the "Redacted Confidential Filing") to the Commission via ECFS in WC Docket No. 05-25 and RM-10593.[7] The Redacted Confidential Filing and the accompanying cover letter shall be stamped "REDACTED – FOR PUBLIC INSPECTION." The cover letter accompanying the Redacted Confidential Filing shall

[7] If a party is not able to submit a copy of the Redacted Confidential Filing via ECFS, it must submit two copies of the Redacted Confidential Filing to the Secretary's Office along with the appropriately stamped cover letter, as described in this paragraph.

state that the party is filing a redacted version of the filing and shall reference WC Docket No. 05-25 and RM-10593. Each Redacted Confidential Filing shall have the same pagination as the Confidential Filing from which it is derived. To the extent that any page of the Confidential Filing contains any type of Confidential Information, only the Confidential Information (of whatever type) may be redacted and the page of the unredacted Confidential Filing shall clearly distinguish among the various types of Confidential Information and the non-confidential information. Two copies of each Confidential Filing and the accompanying cover letter must be delivered, as directed by Commission staff, to Christopher S. Koves, Christopher.Koves@fcc.gov, (202) 418-8209, Pricing Policy Division, Wireline Competition Bureau, Federal Communications Commission, 445 12th Street, S.W., Washington, D.C. 20554. Parties should not provide courtesy copies of pleadings containing Highly Confidential Information to Commission staff unless the Bureau so requests, and any such courtesy copies shall be submitted under seal.

11. *Non-Disclosure of Confidential Information and Highly Confidential Information*. Except with the prior written consent of the Submitting Party or as provided under this Data Collection Protective Order, Confidential Information and Highly Confidential Information may not be disclosed further.

12. *Protection of Stamped Confidential Documents, Stamped Highly Confidential Documents, Confidential Information, and Highly Confidential Information.* A Reviewing Party shall have the obligation to ensure that access to Confidential Information and Highly Confidential Information (including Stamped Confidential Documents and Stamped Highly Confidential Documents) is strictly limited as prescribed in this Data Collection Protective Order. A Reviewing Party shall have the further obligation to ensure that Confidential Information and Highly Confidential Information are used only as provided in this Data Collection Protective Order.

13. *Requests for Additional Disclosure*. If any person requests disclosure of Confidential or Highly Confidential Information outside the terms of this Data Collection Protective Order, such a request will be treated in accordance with sections 0.442 and 0.461 of the Commission's rules.

14. *Client Consultation*. Nothing in this Data Collection Protective Order shall prevent or otherwise restrict Counsel from rendering advice to their clients relating to the conduct of this proceeding and any subsequent judicial proceeding arising therefrom and, in the course thereof, relying generally on examination of Confidential Information or Highly Confidential Information to which they have access under this Data Collection Protective Order; *provided, however*, that in rendering such advice and otherwise communicating with such clients, Counsel shall not disclose Confidential Information or Highly Confidential Information.

15. *No Waiver of Confidentiality*. Disclosure of Confidential or Highly Confidential Information as provided herein by any person shall not be deemed a waiver by any Submitting Party of any privilege or entitlement to confidential treatment of such Confidential or Highly Confidential Information. Reviewing Parties, by viewing this material, agree: (1) not to assert any such waiver; (2) not to use Confidential or Highly Confidential Information to seek disclosure in any other proceeding; and (3) that accidental disclosure of Confidential or Highly Confidential Information by a Submitting Party shall not be deemed a waiver of any privilege or entitlement as long as the Submitting Party takes prompt remedial action.

16. *Subpoena by Courts, Departments*, *or Agencies*. If a court, or a federal or state department or agency issues a subpoena for or orders the production of Stamped Confidential Documents, Stamped Highly Confidential Documents, Confidential Information, or Highly Confidential Information that a party has obtained under terms of this Data Collection Protective Order, such party shall promptly notify each Submitting Party of the pendency of such subpoena or order. Consistent with the independent authority of any court, department or agency, such notification must be accomplished such that the Submitting Party has a full opportunity to oppose such production prior to the production or disclosure of any Stamped Confidential Document, Stamped Highly Confidential Document, Confidential Information, or Highly Confidential Information.

17. *Violations of the Data Collection Protective Order.* Should a Reviewing Party violate any of the terms of this Data Collection Protective Order, such Reviewing Party shall immediately convey that fact to the Commission and to the Submitting Party. Further, should such violation consist of improper disclosure of Confidential or Highly Confidential Information, the violating person shall take all necessary steps to remedy the improper disclosure. The Commission retains its full authority to fashion appropriate sanctions for violations of this Data Collection Protective Order, including but not limited to suspension or disbarment of Counsel or Consultants from practice before the Commission, forfeitures, cease and desist orders, and denial of further access to Confidential or Highly Confidential Information in this or any other Commission proceeding. Nothing in this Data Collection Protective Order shall limit any other rights and remedies available to the Submitting Party at law or in equity against any person using Confidential or Highly Confidential Information in a manner not authorized by this Data Collection Protective Order.

18. *Termination of Proceeding*. The provisions of this Data Collection Protective Order shall not terminate at the conclusion of this proceeding. Within two weeks after conclusion of this proceeding and any administrative or judicial review, Reviewing Parties shall destroy or return to the Submitting Party Stamped Confidential Documents and Stamped Highly Confidential Documents and all copies of the same. No material whatsoever containing or derived from Confidential and Highly Confidential Information may be retained by any person having access thereto, except Outside Counsel may retain, under the continuing strictures of this Data Collection Protective Order, two copies of pleadings (one of which may be in electronic format) prepared in whole or in part by that party that contain Confidential or Highly Confidential Information, and one copy of orders issued by the Commission or Bureau that contain Confidential or Highly Confidential Information. All Counsel shall certify compliance with these terms and shall deliver such certification to Counsel for the Submitting Party not more than three weeks after conclusion of this proceeding. The provisions of this paragraph regarding retention of Stamped Confidential Documents and Stamped Highly Confidential Documents and copies of the same and Confidential and Highly Confidential Information shall not be construed to apply to the Commission or its staff.

19. *Questions*. Questions concerning this Data Collection Protective Order should be addressed to Christopher S. Koves, Christopher.Koves@fcc.gov, (202) 418-8209, Pricing Policy Division, Wireline Competition Bureau, Federal Communications Commission, 445 12th Street, S.W., Washington, D.C. 20554.

20. *Authority*. This Data Collection Protective Order is issued pursuant to sections 4(i), 5, 201-205, 211, 215, 218, 219, 303(r), and 332 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 154(i), 155, 201-205, 211, 215, 218, 219, 303(r), and 332, Section 4 of the Freedom of Information Act, 5 U.S.C. § 552(b)(4), and authority delegated under section 0.291 of the Commission's rules, 47 C.F.R. § 0.291, and the *Data Collection Order*, 27 FCC Rcd 16318, 16340, para. 52 (2012), and is effective upon its adoption.

FEDERAL COMMUNICATIONS COMMISSION

Deena M. Shetler
Associate Chief
Wireline Competition Bureau

APPENDIX B

Highly Confidential Information

WC Docket No. 05-25
RM-10593

As specified in paragraph 1 of the Data Collection Protective Order, only information set forth in this Appendix and that otherwise meets the definition of Highly Confidential Information may be designated as Highly Confidential Data or Highly Confidential Information. Submitting Parties retain the right to request Confidential treatment of data and information submitted in this proceeding by so designating consistent with paragraphs 3 and 11 of the Data Collection Protective Order. This Appendix will be updated as necessary.[1]

Highly Confidential Information that is Highly Confidential Data

Data may be designated as Highly Confidential Data pursuant to the Data Collection Protective Order only if it contains information regarding:

1. The *Locations* that *Providers* serve with last-mile facilities and the nature of those facilities. (Questions II.A.3-4, II.B.2-3)
2. The location of companies' fiber network routes, including the locations of all *Nodes* used to interconnect with third party networks and the year that each *Node* went live. (Question II.A.5)
3. The date that a party first provided a *Connection* to a *Location*, including whether the party originally supplied the *Location* over an *Unbundled Network Element* ("*UNE*") and, if so, when the party switched to using a Connection that it owned or leased under an *Indefeasible Right of Use* ("*IRU*") agreement. (Question II.A.6)
4. The location of a company's collocations. (Question II.A.7)
5. Information about Requests for Proposals ("RFPs"), including descriptions of RFPs for which a party was selected as the winning bidder, descriptions of RFPs for which a party submitted unsuccessful competitive bids, and the business rules companies take into consideration to determine whether to submit a bid in response to an RFP. (Question II.A.11)
6. The rates or charges associated with channel terminations or transport facilities, including adjustments, rebates, and true-ups, and information from which, whether alone or in combination with other confidential or non-confidential information, such rates or charges could be inferred. (Questions II.A.12-14, II.B.4-6)
7. Information on *Revenues* from the sale of *Dedicated Service*. (Questions II.A.15-17, II.B.8-10, II.B.12(q))
8. The number of customers purchasing *Dedicated Services* pursuant to *One Month Term Only Rates*, in total and disaggregated by customer category and service type. (Question II.B.11)

[1] For ease of reference, each category is followed by a parenthetical identifying the data collection question(s) that request the type of information described by that category. Capitalized and italicized terms refer to the definitions in the data collection. *Special Access for Price Cap Local Exchange Carriers; AT&T Corporation Petition for Rulemaking to Reform Regulation of Incumbent Local Exchange Carrier Rates for Interstate Special Access Services*, WC Docket No. 05-25, RM-10593, Order on Reconsideration, DA 14-1327, App. A (Wireline Comp. Bur. rel. Sept. 15, 2014).

9. The number of customers associated with a *Tariff Plan* or *Contract-Based Tariff*, in total and disaggregated by customer category and service type, including the number of new subscribers to a *Tariff Plan* or *Contract-Based Tariff*. (Question II.B.12(s))
10. Information relating to data submitted by an entity in connection with the State Broadband Initiative Grant Program that would reveal the areas where an entity offers *Best Efforts Business Broadband Internet Access Service* and the prices offered for *Best Efforts Business Broadband Internet Access Services*. (Questions II.C.1(b), II.C.1(b)(i)-(ii))
11. Information on the number and location of a company's cell sites and the backhaul facilities used to connect the cell sites to a carrier's network. (Questions II.E.1-2)

Other Highly Confidential Information

Information may be designated as Highly Confidential Information pursuant to the Data Collection Protective Order only if it contains information regarding:

1. Non-specific information on whether a party or an *Affiliated Company* owns a *Connection*, leases a *Connection* from an entity under an *IRU* agreement, or obtains a *Connection* as a *UNE* to provide a *Dedicated Service*, including whether any of the *Connections* are to a *Location* within an area subject to price cap regulation or within an area where the Commission has granted pricing flexibility. (Questions II.A.2, II.A.9(e)).
2. The business rules and other factors companies take into consideration when deciding whether to self-deploy channel termination and local transport facilities or lease such facilities from a third party, including the geographic areas where a party has built the most *Connections* to *End Users* and whether and how business density is incorporated into the party's business rule. (Questions II.A.8, II.A.8(a)-(c)).
3. Data, maps, information, marketing materials, and/or documents identifying those geographic areas where a party or an *Affiliated Company* planned to advertise or market *Dedicated Services* within twenty-four months of the time periods specified in the data collection. (Question II.A.10)
4. The number of customers who fail to meet any *Volume Commitment* or *Term Commitment* required to retain a discount or *Non-Rate Benefit*. (Question II.B.12(t))
5. The terms of non-tariffed agreements with an *ILEC*, *End User* or *Competitive Provider* for the purchase of *Dedicated Services* (*e.g.*, parties to the agreement, effective date of the agreement, services purchased). (Questions II.B.13, II.F.14)
6. Information relating to a *Provider's* short term and long-range promotional and advertising strategies and objectives for winning new customers for *Dedicated Services* or retaining new customers for *Dedicated Services*. (Question II.D.1)
7. Expenditures on *Dedicated Services* and expenditures under certain rate structures and discount plans, including purchases made pursuant to *Tariff Plans*, *Contract-Based Tariffs*, and non-tariffed agreements. (Questions II.F.2-7)
8. Information about the steps a *Purchaser* undertakes to change *Transport Providers* while keeping its *End User Channel Terminations* with its existing *Provider*; specifically, the number of circuits moved (or requested to be moved) and information about the rates for the *End User Channel Terminations* purchased from the existing *Provider* or rates paid for *Transport Service* while the change in service was pending. (Question II.F.9(a), F.9(d), F.9(e))
9. Information about the purchase of circuits pursuant to a *Tariff* solely for the purpose of meeting a *Prior Purchase-Based Commitment* required for a discount or to obtain a *Non-Rate Benefit* from a *Provider*; specifically, the name of *Provider* providing the circuits at issue, a description of the *Prior Purchase-Based Commitment*, and the number of unnecessary or unused circuits purchased

and expenditures for unnecessary or unused circuits. (Questions II.E.11(a)-(b), (d)-(g) and II.F.10(a)-(b), (d)-(g))

10. Information about switching from purchasing *End-User Channel Terminations* from one *Provider* of *Dedicated Services* to another that would reveal the services purchased by a customer or the geographic area where services were purchased. (Question II.F.11)

11. A company's business rule for purchasing circuits at a *One Month Term Only Rate* and the business rationale for that rule. (Question II.F.12)

12. The geographic areas in which a *Purchaser* buys *Dedicated Services* to avoid penalties or obtain plan benefits under a *Tariff Plan* or *Contract-Based Tariff*, and the geographic areas where the *Purchaser* would have bought *Dedicated Services* from a different *Provider* if not for the plan requirements. (Questions II.F.13(i), II.F.13(k)(i)-(ii), II.F.13(l)(i), II.F.13(m)(i)-(ii), II.F.13(n)(i)-(ii), and II.F.13(o)(i)-(ii))

Data and Information Eligible for Highly Confidential Treatment

To the extent your response to the questions referenced below contains the following categories of information, we will consider such data or information eligible for Highly Confidential treatment under the Data Collection Protective Order:

1. The business justification for the *Term* or *Volume Commitments* associated with any *Tariff* or agreement *Competitive Providers* or *ILECs* offer or have in effect with a customer for the sale of *Dedicated Services.* (Questions II.A.19, II.B.12(r))

2. The rates paid for *End User Channel Terminations* by *Purchasers* that are mobile wireless service providers that purchased both *Transport Service* and *End User Channel Terminations* before and after connecting to a new *Transport Provider* while keeping *End User Channel Terminations* with the original *Provider*. (Questions II.E.10(d)-(e), II.F.9(d)-(e))

3. Detailed information on the terms and conditions of non-tariffed contracts to which *Purchasers* that are not mobile wireless service providers are a party for the purchase of *Dedicated Services*. (Questions II.E.9, II.F.8)

4. Detailed information on the amount of time it takes to complete the process of connecting *Purchasers* to complete the process of connecting their *End User Channel Terminations* to another *Transport Provider*, including *ILEC's* or *Competitive Provider's* policies or rules explain the transition process. (Questions 11.E.10(b)-(c), II.F.9(b)-(c))

APPENDIX C

Acknowledgment of Confidentiality

WC Docket No. 05-25; RM-10593

I am seeking access to [ ] only Confidential Information or [ ] Confidential and Highly Confidential Information.

I hereby acknowledge that I have received and read a copy of the foregoing Data Collection Protective Order in the above-captioned proceeding, and I understand it.

I agree that I am bound by the Data Collection Protective Order and that I shall not disclose or use Stamped Confidential Documents, Stamped Highly Confidential Documents, Confidential Information, or Highly Confidential Information except as allowed by the Data Collection Protective Order.

I acknowledge that a violation of the Data Collection Protective Order is a violation of an order of the Federal Communications Commission (Commission). I further acknowledge that the Commission retains its full authority to fashion appropriate sanctions for violations of this Data Collection Protective Order, including but not limited to suspension or disbarment of Counsel or Outside Consultants from practice before the Commission, forfeitures, cease and desist orders, and denial of further access to Confidential or Highly Confidential Information in this or any other Commission proceeding.

I acknowledge that nothing in the Data Collection Protective Order limits any other rights and remedies available to a Submitting Party at law or in equity against me if I use Confidential or Highly Confidential Information in a manner not authorized by this Data Collection Protective Order.

I certify that I am not involved in Competitive Decision-Making.

Without limiting the foregoing, to the extent that I have any employment, affiliation, or role with any person or entity other than a conventional private law firm (such as, but not limited to, a lobbying or advocacy organization), I acknowledge specifically that my access to any information obtained as a result of the Data Collection Protective Order is due solely to my capacity as Counsel or Outside Consultant to a party or as a person described in paragraph 9 of the Data Collection Protective Order and agree that I will not use such information in any other capacity.

I acknowledge that it is my obligation to ensure that Stamped Confidential Documents and Stamped Highly Confidential Documents are not duplicated except as specifically permitted by the terms of the Data Collection Protective Order and to ensure that there is no disclosure of Stamped Confidential Documents, Stamped Highly Confidential Documents, Confidential Information, and Highly Confidential Information in my possession or in the possession of those who work for me, except as provided in the Data Collection Protective Order.

I certify that I have verified that there are in place procedures at my firm or office to prevent unauthorized disclosure of Confidential Information and Highly Confidential Information.

Capitalized terms used herein and not otherwise defined shall have the meanings ascribed to them in the Data Collection Protective Order.

Executed this ___ day of _____, 20__.

_____

[Name]
[Position]
[Firm]
[Telephone]