CROWN CASTLE

11/06/2020

Dedicated Internet Access (DIA), Dark Fiber, and Ethernet Services

Prepared for: Ulster BOCES
RFP Number: 21-18
Proposal submitted by: Crown Castle

Jim Nocito
Commercial Account Executive
Crown Castle
900 Corporate Blvd., Suite #2
Newburgh, NY 12550
(845) 458-7741

Finny Connell
Commercial Account Executive
Crown Castle
900 Corporate Blvd., Suite #2
Newburgh, NY 12550
(845) 458-7708

ATTACHMENT "E"

EDUCATION LAW 2-D RIDER

New York State Education Law 2-d was enacted in 2014 to address concerns relative to securing certain personally identifiable information. In order to comply with the requirements of Education Law 2-d, educational agencies and certain third-party contractors who contract with educational agencies must take certain additional steps to secure such data. These steps include enacting and complying with a Parents' "Bill of Rights" relative to Protected Data, ensuring that each third-party contractor has a detailed data privacy plan in place to ensure the security of such data, and that each third-party contractor sign a copy of the educational agency's Parents' Bill of Rights, thereby signifying that the third-party contractor will comply with such Parents' Bill of Rights. This Agreement is subject to the requirements of Education Law 2-d and Vendor is a covered third-party contractor.

In order to comply with the mandates of Education Law 2-d, and notwithstanding any provision of the Agreement between Ulster BOCES and Vendor to the contrary, Vendor agrees as follows:

Vendor will treat "Protected Data" (as defined below) as confidential and shall protect the nature of the Protected Data by using the same degree of care, but not less than a reasonable degree of care, as the Vendor uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third parties. Vendor shall not disclose Protected Data other than to those of its employees or agents who have a need to know such Protected Data under this Agreement. Vendor shall not use Protected Data for any other purposes than those explicitly provided for in this Agreement. All Protected Data shall remain the property of the disclosing party. As more fully discussed below, Vendor shall have in place sufficient internal controls to ensure that Ulster BOCES' and/or its participants' Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, CIPA, FERPA, HIPAA and Part 121 of the Regulations of the Commissioner of Education, as it may be amended from time-to-time, if applicable.

"**Protected Data**" includes any information rendered confidential by State or federal law, including, but not limited to student data, student demographics, scheduling, attendance, grades, health and discipline tracking, and all other data reasonably considered to be sensitive or confidential data by Ulster BOCES and/or a participant. Protected Data also includes any information protected under Education Law 2-d including, but not limited to:

> "Personally identifiable information" from student records of Ulster BOCES and/or its Participants as that term is defined in §99.3 of the Family Educational Rights and Privacy Act (FERPA),
>
> -AND-
>
> Personally identifiable information from the records of Ulster BOCES and/or its participants relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §3012-c.

Vendor and/or any Subcontractor, affiliate, or entity that may receive, collect, store, record or display any Protected Data shall comply with New York State Education Law § 2-d. As applicable, Vendor agrees to comply with Ulster BOCES' policy(ies) on data security and privacy. Vendor shall promptly reimburse Ulster BOCES and/or its participants for the full cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of Protected Data by Vendor, its Subcontractors, and/or assignees. In

the event this Agreement expires, is not renewed or is terminated, Vendor shall return all of Ulster BOCES' and/or its participants' data, including any and all Protected Data, in its possession by secure transmission.

Data Security and Privacy Plan

Vendor and/or any Subcontractor, affiliate, or entity that may receive, collect, store, record or display any of Ulster BOCES' and/or its participant's Protected Data, shall maintain a Data Security and Privacy Plan that includes the following elements:

1. A provision incorporating the requirements of Ulster BOCES' Parents' Bill of Rights for data security and privacy and Supplemental Information for Third Party Contractors, to the extent that any of the provisions in the Bill of Rights applies to Vendor's possession and use of Protected Data pursuant to this Agreement.

2. An outline of how all state, federal, and local data security and privacy contract requirements will be implemented over the life of the contract, consistent with Ulster BOCES' policy on data security and privacy.

3. A provision specifying the administrative, operational and technical safeguards and practices in place to protect personally identifiable information that Vendor will receive under the contract.

4. A provision specifying how officers or employees of Vendor and its assignees who have access to Protected Data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access.

5. An outline of how Vendor will ensure that any Subcontractors, persons or entities with which Vendor will share Protected Data, if any, will abide by the requirements of Vendor's policy on data security and privacy, and the contractual obligations with respect to Protected Data set forth herein.

6. A provision specifying how Vendor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify Ulster County BOCES.

7. A provision specifying whether Protected Data will be returned to Ulster County BOCES, transitioned to a successor contractor, at the District's option and direction, deleted or destroyed by the Vendor when the contract is terminated or expires.

VENDOR DATA PRIVACY AND SECURITY PLAN

1. [VENDOR MUST INCLUDE COPY OF ITS DATA AND PRIVACY PLAN]

2. [VENDOR MUST PROVIDE A **SIGNED** COPY OF Ulster BOCES' BILL OF RIGHTS]

ATTACHMENT "F"

PARENTS BILL OF RIGHTS
PARENTS BILL OF RIGHTS - DATA PRIVACY & SECURITY

Ulster BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law §2-d, Ulster BOCES wishes to inform the community of the following:

1. A student's personally identifiable information cannot be sold or released for any marketing or commercial purposes.

2. Parents have the right to inspect and review the complete contents of their child's education record.

3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.

4. A complete list of all student data elements collected by the State is available for public review here, or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to:

Ulster BOCES
175 Route 32 North
New Paltz, New York 12561

or

Chief Privacy Officer
New York State Education Department
89 Washington Avenue
Albany, New York 12234

Complaints may also be directed to the Chief Privacy Officer (CPO) via email at CPO@mail. nysed.gov

6. The District Superintendent shall develop regulations to ensure compliance with all state and federal laws and regulations regarding the protection and security of student data and teacher or principal data.

SUPPLEMENTAL INFORMATION REGARDING THIRD PARTY CONTRACTORS

In the course of complying with its obligations under the law and providing educational services, Ulster BOCES has entered into agreements with certain third-party contractors. Pursuant to such agreements, third-party contractors may have access to "student data" and/or "teacher or principal data," as those terms are defined by law.

Each contract Ulster BOCES enters into with a third party contractor where the third party contractor receives student data or teacher or principal data will include the following information:

1. The exclusive purposes for which the student data or teacher or principal data will be used by the third party contractor;

2. How the third party contractor will ensure that the subcontractors, persons or entities with whom the third party contractor will disclose the student data or teacher or principal data, if any, will abide by data protection and security requirements;

3. The duration of the contract, including when the agreement expires and what happens to the student data or teacher or principal data upon expiration of the agreement;

4. If and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected;

5. Where the student data or teacher or principal data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected and data security and privacy risks mitigated; and address how the data will be protected using encryption while in motion and at rest.

6. How the data will be protected using encryption while in motion and at rest.

Proposer Signature: Douglas C. VanDuzer

Date: October 30, 2020

CUSTOMER PROPRIETARY

NETWORK INFORMATION

("CPNI")

PROTECTION POLICY

Crown Castle Fiber, LLC

Crown Castle Fiber LLC ("Crown Castle Fiber") requires all employees, contractors, agents, affiliates and partners, including sales and marketing agents, to protect the confidentiality of customer information. The Federal Communications Commission ("FCC') may consider customer information obtained by Crown Castle Fiber by virtue of its provision of telecommunications service CPNI, and be subject to legal protection under Federal law and regulations. Crown Castle Fiber supports these laws and regulations, and requires that all employees, contractors, agents, affiliates and partners comply with this CPNI Protection Policy and procedures set forth herein.

See Glossary at the end of this document for meanings of certain capitalized terms.

SUMMARY

CPNI includes:

- information about circuits that we provide to our customers (capacity, endpoints, and so forth);
- information about dark fiber that we provide to our customers (for example, number of strands, physical route); and,
- billing and usage information on the switched services we provide (generally, through resale or UNE arrangements with the incumbent local exchange companies).

How do we protect CPNI?

- Crown Castle Fiber will not share CPNI unavailable publicly with individuals outside of the customer's organization without the approval of the customer. Notwithstanding, Crown Castle Fiber may use CPNI to resolve technical issues with the customer, provision services, and bill for services.
- In addition to the foregoing, those authorized with access to CPNI may use the customer's CPNI:
    - To market services within the current group of services to which the customer already subscribes.
    - To market Communications-Related services outside of the current group of services that the customer buys, provided the customer consented to use of the CPNI for such marketing. Such consent can be obtained via an **opt-out** letter.
    - To market non-Communications-Related products and services to the customer, only if the customer consented to the use of the CPNI for such purposes through the use of an **opt-in** letter.
    - Crown Castle Fiber will not share CPNI with joint venture partners and independent contractors unless the customer consented to the use of the CPNI through an **opt-in** letter, sent to the customer only by Crown Castle Fiber.
    - Currently, 3 different groups of service apply to Crown castle Fiber, including: long-haul, metro and wireless services. The wireless service application includes instances wherein Crown Castle Fiber provides a wireless connection, and excludes cases wherein the customer provides wireless services and Crown Castle Fiber simply provides capacity or dark fiber.

How do we document and ensure our protection of CPNI?

- Crown Castle Fiber shall distribute this CPNI Protection Policy to all applicable Crown Castle Fiber employees during each calendar year. Each employee must confirm that he or she has read and understands the CPNI Protection Policy; failure to do so may result in disciplinary action up to and including termination. In addition, Crown Castle Fiber shall provide training regularly to ensure that all authorized individuals or employees with access to CPNI understand the CPNI Protection Policy.
- All discussions with customers involving the marketing of new services shall be documented in CRM.
- All requests for CPNI from any person or entity shall be handled in accordance with this CPNI Protection Policy.

WHAT IS CPNI?

CPNI is defined by Federal statute:

The term "Customer Proprietary Network Information" means ---

(A) information that relates to the quantity, technical configuration, type, destination, location and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and

(B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier;

----- except that such term does not include subscriber list information.

47 United States Code § 222(h)(1).

CPNI comprises most information Crown Castle Fiber collects relating to a customer arising out of the purchase of telecommunications services from Crown Castle Fiber, including:

- Information about the ***types*** of service a customer buys, such as the technical configuration, destination and location of services a customer purchases from Crown Castle Fiber. This may include design layout reports, service addresses, originating and terminating locations, circuit speed and capacity, etc.;

- information about the ***amount*** of service a customer purchases from Crown Castle Fiber. For example, this may include the number of lines, circuits, calls, minutes, or the amount of equipment, subscribed to by the customer;

- information about a customer's ***usage*** of telecommunications services, including numbers called, calls received, and optional features utilized; and,

- information contained in a bill sent to the customer by Crown Castle Fiber.

CPNI does *not* include:

- Information obtained by Crown Castle Fiber outside its carrier-customer relationship with the customer. For example, market information that Crown Castle Fiber may purchase from an outside source which happens to include data considered CPNI concerning one of Crown Castle Fiber's customers. However, Crown Castle Fiber shall handle all CPNI obtained from a Crown Castle Fiber affiliate also providing service to a customer as CPNI and handle according to the CPNI Protection Policy.

- Subscriber List Information. This is a defined term under Federal law, and it means any information of a Crown Castle Fiber subscriber (such as name, address, telephone number

or classification) that the company or an affiliate has published, caused to be published, or accepted for publication in a directory.

RESTRICTIONS ON USE OF CPNI

How may CPNI be used *without* the customer's approval?

- CPNI may always be used to provide the telecommunications service that the customer has purchased (such as customer service and repair), or to provide services necessary to, or used in, the provision of such telecommunications services, including the publishing of directories.

- Crown Castle Fiber may use CPNI, without notice or approval, to bill and collect for services rendered, and to protect the Crown Castle Fiber's rights and property (including fraud control).

- Crown Castle Fiber may use Aggregate Customer Information without restriction. However, if the Crown Castle Fiber uses Aggregate Customer Information for purposes other than providing telecommunications services, Crown Castle Fiber will make the same aggregate information available to other parties upon request, on reasonable and non-discriminatory terms and conditions.

- Crown Castle Fiber may use CPNI for wire line service without notice or customer approval, when providing customer premise equipment, call answering, voice mail or messaging, voice storage and retrieval services, fax storing and forwarding services and protocol conversion.

- CPNI may be used, without notice or approval, for marketing Crown Castle Fiber's services within a category of Crown Castle Fiber's services to which the customer already subscribes. The FCC recognizes three (3) categories of telecom services: local, inter-exchange and CMRS (mobile wireless) service. Therefore, if a customer already subscribes to Crown Castle Fiber's local service, the company may, without notice or approval, use that customer's CPNI for the purpose of marketing additional local services.

- CPNI may be used to assist with any inbound telemarketing or administrative service customer support for the duration of the customer's call, if the customer orally approves use of CPNI in this manner.

How may CPNI be used *with* the customer's approval?

- Crown Castle Fiber may use CPNI to market it's Communications-Related Services, and may disclose to Crown Castle Fiber's affiliates, as well as the Crown Castle Fiber's third-party agents providing Communications-Related Services, if the customer received notice, and provides approval by the "opt-out" procedure. Specific requirements apply as to how customer receives notices, and the procedures pertaining to "opt-out" approval must be closely observed.

- Crown Castle Fiber generally prohibits disclosure of CPNI to unrelated third parties. However, Crown Castle Fiber may disclose CPNI to independent contractors and joint

venture partners, as well as to unrelated third parties and affiliates that *do not* provide Communications-Related Services, if the customer consents through the "opt-in" procedure.

- **When is Crown Castle Fiber *required* to disclose CPNI?**

- Crown Castle Fiber must provide CPNI to any person designated by the customer, upon receipt of an affirmative written request from the customer.

- Crown Castle Fiber must disclose CPNI when required by law. All requests for CPNI from law enforcement personnel will be handled by Crown Castle Legal Department. If you receive a request (written or oral) from any person claiming to be law enforcement personnel, please forward the request to the Crown Castle Legal Department. A request for CPNI includes, but is not limited to, a request for a particular customer or customers' call records. A request from law enforcement personnel may come from a federal or state law enforcement agency, including, but not limited to, the United States Department of Justice, the Federal Bureau of Investigation, the FCC, and the policy department. For purposes of this category, law enforcement personnel also include local state agencies. The Crown Castle Legal Department will review all requests from law enforcement personnel.

- Crown Castle Fiber shall not release any CPNI to any law enforcement personnel or to any person (other than the customer) claiming a right to the information absent a validly issued written subpoena. Crown Castle Fiber shall require any person or entity requesting CPNI orally to reduce the request to writing and direct that request to the senior attorney. All requests for CPNI from any person other than the customer or law enforcement personnel also will be handled by the senior attorney, including, but not limited to, requests from an attorney claiming to have a valid subpoena for the information. If you receive a request for CPNI (written or oral) from any person other than the customer, please forward the request to the Crown Castle Legal Department.

OBTAINING APPROVAL FROM A CUSTOMER TO USE CPNI

Opt-out

- The "opt-out" approval method requires that the customer receive an individual notice (by written or electronic means) that Crown Castle Fiber intends to use the customer's CPNI. Such notices must be sent by Crown Castle Fiber for the customer's approval thirty (30) days in advance of the intended use of CPNI (thirty-three (33) days for notices sent by mail). If the customer communicates to Crown Castle Fiber that use of the CPNI is not approved, the company will honor that customer's decision to "opt-out." In limited cases, oral approvals may be allowed, as described below in the section entitled *Special Requirements Applicable to One-Time Oral Notices to Customers.*

- If Crown Castle Fiber elects to send opt-out notices by e-mail, the customer must previously have agreed to receive e-mails regarding the service account. The subject line of the e-mail must clearly and accurately identify the topic, and the customer must have the option of replying directly to the e-mail. If the e-mail is returned as undeliverable, Crown Castle Fiber may be not use the customer's CPNI until the required notice is given by another means.

- The customer must be able to opt-out at no cost and be able notify Crown Castle Fiber of the decision on a twenty-four (24) hour/ seven (7)-day-per-week basis.

- Opt-out approval must be refreshed every two years by sending a new notice, with a new thirty (30) or thirty-three (33) day waiting period for approval.

Opt-in

- The opt-in method requires Crown Castle Fiber to obtain from the customer an affirmative, express consent--in oral, electronic or written form--allowing the requested CPNI usage, disclosure or access, after receiving appropriate notification.

- Although customer approvals under the opt-in method may be obtained orally, Crown Castle Fiber allows oral approvals only with prior written authorization received from the customer and confirmation of same by Crown Castle Fiber management. If oral approval is received, the burden will rest with Crown Castle Fiber to demonstrate that the customer received all of the information required in writing, and gave the necessary approval.

Notice Requirements Applicable to both the Opt-in and Opt-out Methods of Approval

- Notices to customers must be clearly written, legible, and provide sufficient information to enable the customer to make an informed decision to allow or deny use of CPNI. Crown Castle Fiber must define CPNI for the customer, name the CPNI at issue, disclose the the proposed use by Crown Castle Fiber, and identify specific entities to receive the CPNI upon approving the release of the CPNI. Although the notice may advise the customer that use or disclosure of CPNI will enhance Crown Castle Fiber's ability to provide services to the customer, the notice must also state that the customer has the right, and Crown Castle Fibe has the duty under Federal law, to protect the confidentiality of CPNI. The customer must be informed of his or her right to deny or later withdraw approval of Crown Castle Fiber's proposed use of CPNI, and also be advised of the precise steps that must be taken in order to grant or deny approval of such use. Customers must be notified that denial of access to CPNI will not affect the provision of any services to which the customer subscribes.

Special Requirements Applicable to One-Time Oral Notices to Customers

In general, one-time oral notices are appropriate when Crown Castle Fiber made a one-time inbound or outbound telephone contact with the customer and access to CPNI is useful to analyze the customer's existing service. In such cases, Crown Castle Fiber may use oral notices to obtain limited, one time use of CPNI only for the duration of the call, without regard to whether Crown Castle Fiber uses opt-out or opt-in approval process with respect to that customer. When using the one time oral notice method, the customer must be advised of the same information that otherwise provided in a written or electronic notice. However, certain information may be omitted from the oral notice, if it is clearly inapplicable, including: (a) notice that CPNI will be shared with affiliates or third parties; (b) the specific steps are necessary to approval or restrict use of CPNI; and (c) previous opt-out decisions require no further action to maintain the opt-out election. Notation should be made in the customer's record of any one-time oral notice to the customer and the customer's acceptance or rejection of one-time use of CPNI.

HOW TO VERIFY A CUSTOMER'S APPROVAL AND OBTAIN SUPERVISORY APPROVAL FOR PROPOSED OUTBOUND MARKETING EFFORTS

CUSTOMER APPROVAL DATABASE

- Crown Castle Fiber maintains a database that identifies whether or not a customer has given approval for access to its CPNI. Crown Castle Fiber obligates all applicable employees, agents, and affiliates, including sales and marketing agents, to review the Customer Approval database before using, disclosing or permitting access to a customer's CPNI.

- Crown Castle Fiber prohibits all employees, agents, and affiliates of Crown Castle Fiber, including sales and marketing agents, from using, disclosing or permitting access to CPNI of any customer failing to appear on the list in the database as having given approval. Disciplinary action may result from violation of this prohibition up to and including termination.

- Crown Castle Fiber prohibits employees, agents, and affiliates, including sales and marketing agents, from using, disclosing, or permitting access to the CPNI database to joint venture partners and independent contractors except on a customer-specific basis, and only if the customer consented to the sharing of CPNI with Crown Castle Fiber's independent contractors and joint venture partners for marketing purposes.

- Independent contractors and joint venture partners are permitted to use CPNI for marketing purposes only to the extent a customer consented to the sharing of CPNI with Crown Castle Fiber's independent contractors and joint venture partners for marketing purposes. Independent contractors and joint venture partners shall only use CPNI in as authorized by the customer, in accordance with the safeguards set forth in the contract with Crown Castle Fiber, and consistent with the CPNI Protection Policy.

- Crown Castle Fiber requires all employees, agents, and affiliates, including sales and marketing agents, to obtain supervisory review before making any request to a customer to use, disclose or permit access to CPNI. The review shall ensure adherence to the requirements of this CPNI Protection Policy statement. As an exception, a sales representative may request that the customer authorize the use, disclosure, or access to CPNI limited to the duration of a specific customer contact.

- All Crown Castle Fiber joint venture partners and independent contractors must request approval from the Legal Department to obtain access to the CPNI database. Crown Castle fiber will provide access on a project by project basis, and only for customers who have consented to the joint venture partner and independent contractor use of CPNI for the particular purpose for which approval is sought.

CUSTOMER VERIFICATION AND RELEASE OF CPNI

- Each customer will be assigned a designated point of contact at Crown Castle Fiber. The designated point of contact will handle all of the customer's sales and service requests. Each customer will designate a point of contact responsible for working with the Crown Castle Fiber point of contact. Crown Castle Fiber will verify all incoming calls. Crown Castle Fiber representatives will know each of their customer's point of contacts personally. If Crown Castle Fiber does not recognize the point of contact (for example, by voice), then Crown Castle Fiber must ensure that it is speaking with the point of contact through other verification means, including, but not limited to, obtaining the person's name, company address, and specific information regarding the company's services. If the customer is unable to verify any of the requested details, then the Crown Castle Fiber point of contact may not proceed with the call. In these situations, the Crown Castle Fiber point of contact may call the customer at its telephone number of record to discuss the account, but may not release any information during the preceding in-bound call.

- Crown Castle Fiber does not generate call detail information, as that term is defined in the FCC's rules (and listed at the end of this document in the Glossary). If Crown Castle Fiber subsequently provides services generating call detail information, then such information will not be released over the phone, but only will be released to the customer's address of record. Under no circumstances will any customer information be released except to the customer's address of record.

ACCOUNT CHANGES

All account changes must be in writing and must be made in accordance with the customer's Master Service Agreement and/or Service Agreement with Crown Castle Fiber.

CONFIDENTIALITY AGREEMENTS WITH CONTRACTORS AND JOINT VENTURERS

Crown Castle Fiber will typically not share CPNI outside of the company.

If it becomes necessary for Crown Castle Fiber to share CPNI with a partner, contractor or agent, Crown Castle Fiber will do so only after that person or entity has entered into a confidentiality agreement with Crown Castle Fiber. Any such arrangements require the specific approval of the senior attorney. The confidentiality agreement must include the following:

- Require that the partner, contractor or agent use the CPNI only for the purpose of marketing or providing the Communications-Related Services for which it was provided;

- Disallow the partner, contractor or agent from using, allowing access to or disclosing the CPNI to any other party, unless required to make such disclosure under force of law; and,

- Require that the partner, contractor or agent have appropriate protections in place to ensure the ongoing confidentiality of the customer's CPNI.

All confidentiality agreements shall be reviewed by the Legal Department.