Inteserra
CONSULTING GROUP

151 Southhall Lane, Ste 450
Maitland, FL 32751
P.O. Drawer 200
Winter Park, FL 32790-0200
www.inteserra.com

February 8, 2019
Via ECFS Filing

Ms. Marlene H. Dortch, FCC Secretary
Federal Communications Commission
9050 Junction Drive
Annapolis Junction, MD 20701

RE: Telnet Worldwide, Inc.
EB Docket No. 06-36; CPNI Certification for CY2018

Dear Ms. Dortch:

Attached for filing is the Calendar Year 2018 CPNI Compliance Certification and Statement of CPNI Procedures and Compliance as required by 47 C.F.R. Section 64.2009 (e) submitted on behalf of Telnet Worldwide, Inc.

Any questions you may have regarding this filing should be directed to my attention at 407-740-3002 or via email to cwightman@inteserra.com. Thank you for your assistance in this matter.

Sincerely,

/s/Connie Wightman

Connie Wightman
Consultant

tms: FCCx1901

Enclosures
CW/im

ANNUAL 47 C.F.R. § 64.2009(e) OFFICER'S CERTIFICATION OF CUSTOMER PROPRIETARY NETWORK INFORMATION (CPNI) COMPLIANCE
EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2018:	Covering calendar year 2018
Name of company(s) covered by this certification:	TelNet Worldwide, Inc.
Form 499 Filer ID:	822684
Name of signatory:	Mark Iannuzzi
Title of signatory:	President

1. I, Mark Iannuzzi, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. §64.2001 *et seq.*

2. Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in §64.2001 *et seq.* of the Commission's rules.

3. The company has not taken actions (*i.e.*, proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

4. The company has not received customer complaints in the past year concerning the unauthorized release of CPNI.

5. The company represents and warrants that the above certification is consistent with 47 C.F.R. §1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Mark Iannuzzi, President
TelNet Worldwide, Inc.

2/7/19
Date:

Attachments:
Accompanying Statement explaining CPNI procedures
Explanation of actions taken against data brokers (not applicable, see Statement)
Summary of customer complaints (not applicable, See Statement)

Statement of CPNI Procedures and Compliance
TelNet Worldwide, Inc.

Use of CPNI

TelNet Worldwide, Inc. ("TelNet") does not use or permit access to CPNI to market any services outside of the total service approach as specified in 47 CFR §64.2005. If TelNet elects to use CPNI in a manner that does require customer approval, it will follow the applicable rules set forth in 47 CFR Subpart U, including the institution of operational procedures to ensure that notification is provided and customer approval is obtained before CPNI is used or disclosed.

PROTECTION OF CPNI

TelNet has put into place processes to safeguard its customers' CPNI, including call detail information, from improper use or disclosure by employees; and to discover and protect against attempts by third parties to gain unauthorized access to customer CPNI. These processes include identification of CPNI retained by the company, where it resides and who has access to it.

TelNet ensures that all access to CPNI be approved by a supervisor with knowledge of the FCC's CPNI requirements. TelNet has instituted training procedures and a corresponding disciplinary process to ensure that its personnel understand and comply with restrictions regarding the use and disclosure of, and access to, CPNI. Training includes providing employees with a copy of the FCC's rules regarding CPNI, description and examples of CPNI and pretexting, written policies and procedures for handling CPNI inquiries. All personnel and vendors with access to CPNI are required to sign a confidentiality agreement and acceptable use policy statement. TelNet provides access to CPNI policies on its intranet so that all employees have access to the proper methods of maintaining CPNI confidentiality.

TelNet maintains a record of all sales and marketing campaigns that use CPNI.

TelNet maintains a record of all instances where CPNI was disclosed or provided to third parties, or where third parties where allowed access to CPNI.

DISCLOSURE OF CALL DETAIL OVER PHONE

TelNet has instituted authentication procedures to safeguard the disclosure of call detail over the telephone. TelNet's authentication procedures do not require the use of readily available biographical information or account information as defined by the FCC. TelNet authenticates customers by requiring the customer to establish a password for this purpose. All customers are required to establish a password without the use of readily available biographical information or account information if they want to receive call detail over the telephone. If the appropriate password is not provided, TelNet does not disclose call detail over the telephone.

TelNet does not offer a back-up authentication method, but does allow a customer to reset a lost password. Instructions for resetting the password are provided via mail or email to the address established by the customer of record.

The Company has put into place procedures to notify customers whenever a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record is created or changed without revealing the changed information or sending the notification to the new account information. The Customer of Record is notified by email that the account information has been updated or changed and is given instructions to notify the company's customer service number if the customer believes the account may have been updated or changed in error.

DISCLOSURE OF CPNI ONLINE

Company does not disclose CPNI on-line. If it elects to do so in the future, it will follow the applicable rules set forth in 47 CFR Subpart U, including the implementation of authentication procedures that do not require the use of readily available biographical information or account information and customer notification of account changes.

DISCLOSRE OF CPNI AT RETAIL LOCATIONS

TelNet does not have any retail locations and therefore does not disclose CPNI in-store.

NOTIFICATION TO LAW ENFORCEMENT

TelNet has in place procedures to notify law enforcement in the event of a breach of customers' CPNI and to ensure that customers are not notified of the breach before the time period set forth in the FCC's rules, or, if applicable, when so authorized by law enforcement. TelNet's policy is to notify law enforcement as soon as practicable, but in no event later than seven (7) business days, after a reasonable determination has been made that a breach of its customer's CPNI has occurred. Similarly, TelNet's policy is to notify customers of the breach no sooner than the eighth business day following completion of the notice to law enforcement unless directed by the U.S. Secret Service or the FBI not to so disclose or notify customers. TelNet may extend the period for customer notification pursuant to a written request of a relevant law enforcement agency. TelNet will maintain electronic records of all breaches discovered and notifications made to the USSS and the FBI, and to affected customers.

ACTIONS AGAINST DATA BROKERS

TelNet has not taken any actions against data brokers in the last year.

CUSTOMER COMPLAINTS ABOUT CPNI BREACHES

TelNet did not receive any customer complaints about the unauthorized release of CPNI or the unauthorized disclosure of CPNI in calendar year 2018.

INFORMATION ABOUT PRETEXTERS

TelNet has not developed any information with respect to the processes pretexters are using to attempt to access CPNI but does take steps to protect CPNI by password protecting all CPNI and verification of law enforcement inquiries. When fielding a request from a privileged caller (an attorney, law enforcement, etc.), all such requests are immediately sent to TelNet Compliance Department personnel. Compliance personnel will review each such request and requires proper documentation before detailed information is released.