February 17, 2012
**Via ECFS Filing**

Ms. Marlene H. Dortch, Secretary
Office of the Secretary
Federal Communications Commission
445 12th Street, SW, Suite TW-A325
Washington, DC 20554

**RE: DSI-ITI, LLC**
**CY2011 Annual CPNI Certification Filing**
**EB Docket No. 06-36**

Dear Ms. Dortch:

Attached for filing is the Calendar Year 2011 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 the DSI-ITI, LLC.

Any questions you may have regarding this filing should be directed to my attention at 407-740-3004 or via email to rnorton@tminc.com.

Thank you for your assistance in this matter.

Sincerely,

Robin Norton

Robin Norton
Consultant to DSI-ITI, LLC

cc: Brian Hackett - DSI-ITI, LLC (via email)
file: DSI-ITI, LLC - FCC
tms: FCCx1201

Enclosures
RN/lm

**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 2012: | Covering calendar year 2011 |
| Name of company(s) covered by this certification: | DSI-ITI, LLC |
| Form 499 Filer ID: | 828195 |
| Name of signatory: | Teresa Ridgeway |
| Title of signatory: | Senior Vice President Administration |

1. I, Teresa Ridgeway, 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 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.

Teresa Ridgeway, Senior Vice President Administration
DSI-ITI, LLC

Feb 15, 2012
Date

**Attachment A**
**Statement of CPNI Procedures and Compliance**

**Statement of CPNI Procedures and Compliance**
**For 2011**

**DSI-ITI, LLC**

DSI-ITI, LLC ("DSI-ITI" or "Company") operates solely as a provider of inmate operator services and as such provides pre and post-paid automated operator assisted call completion services to inmates of local, state and federal confinement institutions. The Company provides service via contractual arrangements with inmate facilities, not end users, resulting from responses to public bids from confinement institutions.

DSI-ITI 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 the Company 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 institution of operational procedures to ensure that notification is provided and customer approval is obtained before CPNI is used or disclosed.

DSI-ITI continually educates its employees regarding the appropriate use of CPNI. All DSI-ITI employees are required to sign a Confidentiality Agreement upon hire, which explicitly states that they are not allowed to divulge any proprietary customer data which they may encounter performing their job, including CPNI, during or after their tenure with DSI-ITI. There is a documented company policy guide that outlines the disciplinary procedures should an employee breach this agreement. Resulting disciplinary actions due to breach of the Confidentiality Agreement are handled on a case by case basis, based on the severity of the breach, up to and including immediate termination. All DSI-ITI employees who have access to CPNI are trained annually on the importance of protecting customer data and security. Training includes information and policies on when and how CPNI data can be released and the ramifications of unauthorized release.

The Company directly bills and handles customer service for end user calls it carriers. DSI-ITI Customer Service Representatives ("CSRs") are instructed upon hire not to release any CPNI data over the phone without first authenticating the customer, either via a previously established password or the call back method. There is an annual refresher training for all CSRs. DSI-ITI's CSR application maintains a log of all actions taken by a CSR when handling a specific call. Whether the caller provided their correct password, whether a call back authentication was necessary, whether the caller was setting up a brand new account and set up a new password, is all captured in the log. All calls are also subject to random monitoring by the Customer Service Department supervisors.

Customers may contact DSI-ITI directly to review or discuss the DSI-ITI bill or prepaid account. All of the DSI-ITI Customer Service Representatives (CSRs) are trained on how and when they are allowed to release call detail information. Representatives are informed that they are not to release call detail information, unless the customer can provide the call detail necessary to address their customer service issue, without first authenticating the customer via a pre-established password or calling back to the account phone number on record under any circumstance. The customer provides DSI-ITI with a password of their choosing. DSI-ITI advises the customer that to maximize security, they should choose a password based upon something other than easily obtained biographical or account information. DSI-ITI informs customers, after the password set-up is complete, that this password needs to be provided by the customer before they are allowed to obtain access to any CPNI data via the live Customer Service Department. If a customer is unable to provide the correct password the customer must be re-authenticated via the process outlined above.

The Company's website includes a secure log-in for customers, which requires the use of a customer-selected password. Customers may update account information, review and add to prepaid accounts and pay Company invoices. In the event of an unauthorized disclosure of CPNI, the Company will notify the United States Secret Service, the Federal Bureau of Investigation and the customer in a lawful and timely manner.

Requests for call detail records by law enforcement agencies are only granted if a subpoena is provided.

The Company does not have any retail locations and therefore does not disclose CPNI at in-store locations.

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

The Company did not receive any customer complaints about the unauthorized release of CPNI or call records in calendar year 2011.

The Company has not developed any information with respect to the processes pretexters are using to attempt to access CPNI or call records.