GISB FTTF
Work Paper Detailing EII Actions
Specifically Referencing to FTTF

Items from August 13/14, 1998 EII Meeting

- Regarding Camel Model item nos. 9 and 10, which the EII task force referred to the Future Technology Task Force (FTTF), the EII task force determined that the FTTF should address both EBB and EDM in their recommendations.

- 5.A. "Standard" client configuration is one that allows simultaneous access to multiple industry Web sites. [DEFINITION]
  Note: Issues on add-ins would be forwarded to the Future Technology Task Force (FTTF) as needed.
  GISB standards cannot require the use of a specific commercial product that is not publicly available at no cost.
  The FTTF should further define the term "standard" client configuration.

- 18. The "Customer Activities" navigational link should appear and be labeled as such immediately above Site Map on the Informational Postings Web site. The FTTF should review this standard to determine if secure Web pages (transactional functions) should be available from public Web pages (Informational Postings).
  Vote: Deferred until FTTF provides input on options and security issues.

- **Appendix A**
  The following items have been transferred to the Future Technology Task Force
  7. Minimum technical requirements for access to the transactional Web site are suggested below. These suggestions should be forwarded to FTTF for further development.
  Connection Device 28.8 K or above
  Operating System Multi-threaded & Pre-emptive
  RAM 32Mb or more
  Display Capabilities 800 x 600, 256 colors
  Monitor 12' Laptop 15" Desktop
  Browser Capabilities Support cookies, frames and nested frames, tables and nested tables.
  Examples of User Workstations meeting this criteria:
  Hardware P 200MHz or greater
  Communication Device Direct Connect
  ISDN
  Satellite
  56KB modem
  Operating System Windows 95 or greater
  NT 4.0 or greater
  Solaris 2.6
  System 8
  Browser Microsoft IE 4.0
  Netscape Communicator 4.04 or Netscape Navigator 4.04
  8. FTTF should define security for the transactional Web site after the Business Process Subcommittee has defined the security requirements for access, privacy, integrity and non-repudiation. Security requirements are suggested below that should be forwarded to FTTF for further development.
  At a minimum, the transactional Web page data communications from the browser to the Internet server should be capable of encryption and occur in a protected session. Client-side certificates should not be required. Userid/password authentication is required. The authentication process should be in an encrypted session.

9. FTTF should define any necessary standards for connecting with third party communication networks.
10. FTTF should define redundancy recommendations for Internet connections which allow the TSP to choose the options that are most cost effective for meeting its customer's requirements.

Items from September 3, 1998 EII Meeting

- 51.7 As an instruction to FTTF, IR and Technical, flat files could be exchanged via interactively via the GISB EBB/EDM Customer Activities Website in a manner as follows: The user would click a button indicating a desired upload or download. The system would prompt the user for a filename. The system would acknowledge the status of the exchange. The system could display the results on the screen as if the user had entered all data interactively.

Items from September 17/18, 1998 EII Meeting

- **IV. FTTF Responses to EII Requests Regarding CAMEL Model Items 7, 8, 9, 10 and 18**
  The motion was made to adopt the implementation guide recommendations as provided by the Future Technology Task Force:
  Implementation Guide Content under Customer Activities Sites: Minimum Technical Characteristics of the Client Workstation
  Configuration* Description:
  Hardware:
  CPU >= 166 MHz
  Memory >= 64 MB Physical
  Display Resolution >= 800 x 600
  Operating Systems:
  Multi-threaded and preemptive
  Connection:
  >=56KB (V90)
  Browser Characteristics (includes defined GISB current versions):
  _____
  Features as supported by both Netscape v4.06 and Internet Explorer v4.0 sp1 including:
  - Frames and nested frames
  - Tables and nested tables
  - Style Sheets
  - HTML
  - Cookies
  - JavaScript
  - SSL (40 Bit RSA)
  - Java 1.1.6 Sun JDK (plug-in)
  - ActiveX (Plug-in for Netscape)
  - ICA v4 (Plug-in)

  *configuration shown indicates a minimum except where a specific level is established. "Minimum" implies a level where a reasonable experience for the user may be achieved. These levels also indicate the level that a user may expect that a client has been tested. Results may be less than satisfactory or may preclude use of a site if the user chooses to use anything less than those levels shown.
  Example Configurations of Client for Accessing Customer Activities Sites [1]
  EXAMPLES BELOW REPRESENT A NON-COMPREHENSIVE SET OF CONFIGURATIONS WHICH A CLIENT MAY USE. THIS EXAMPLE LIST IN NO WAY SHOULD BE CONSTRUED AS AN ENDORSEMENT BY GISB OF ANY SPECIFIC PRODUCTS. OTHER PRODUCTS MEETING THE MINIMUM TECHNICAL CHARACTERISTICS OF THE CLIENT WORKSTATION MAY BE USED.
  Hardware:
  CPU: P166 MHz or higher

Memory >= 64 MB Physical
Display Resolution >= 800 x 600
Pointing Device with left and right click capability
Operating Systems:
Windows 95
Windows 98
Windows NT 4.0 service pack 3
Connection:
56KB (V90) modem
ISDN
Direct Connect (T1, Fractional T1…)
Browser:
Netscape Communicator/Navigator v4.06
Microsoft Internet Explorer v4.0 service pack 1
Plug-ins:
Java 1.1.6 Sun JDK (Activator)
ActiveX (Plug-in for Netscape)
ICA v4 (Plug-in)
[1] **Note to EII Task Force from the Future Technology Task Force (9/11/98):**
There is still a review of port numbers possibly needed to be opened on the client-side for certain protocols to be used. We want to arrive at a limited list on which users may rely to be able to access many TSP sites. Along with this, will be some other firewall administration notes addressing items such as applets. We intend to complete this draft in our October FTTF meeting.
[THE ABOVE TECHNICAL CHARACTERISTICS AND EXAMPLES WILL BE REVIEWED FOR TRADEMARK, COPYRIGHT AND OTHER LEGAL CONSIDERATION PRIOR TO NOTICE FOR INDUSTRY COMMENT.] SPECIFIC PRODUCTS SHOULD BE REVIEWED PRIOR TO IMPLEMENTATION FOR YEAR 2000 COMPLIANCE.

7A. Providers of Customer Activities EBB/EDM sites should ensure that the site operates on the "Technical Characteristics of the Client Workstation" described in the appendix of the Electronic Delivery Mechanism Related Standards manual. This appendix, listing examples of hardware and software configurations that providers should meet, should be reviewed and updated by the Future Technology Task Force, at a minimum, by the spring of each year and presented to the GISB Executive Committee for adoption by the June meeting of that group.
VOTE: The motion passed unanimously as a recommended standard. (4.3.x)

The FTTF task force should address a review of port numbers possibly needed to be opened on the client-side for certain protocols to be used. They expect to arrive at a limited list on which users may rely to be able to access many TSP sites. Along with this, will be some other firewall administration notes addressing items such as applets. Any suggested standards regarding this issue will be available for the October 17 EII meeting. [2]

The motion was made to adopt proposed standard 9A
9A. Private network connections to access GISB EDM* sites may be at any point on the TSP firewall boundary at the TSP's discretion on a non-discriminatory basis. The specific type and speed of these connections should be mutually agreed. It is at the discretion of the TSPs on how multiple private network connections should be managed[, so long as such management is done on a non-discriminatory basis]. TSPs are not responsible for any additional security exposures when using these private network connections.
* This includes all GISB standardized Internet communication.
ACTION: The motion was withdrawn for consideration after lunch.

The motion was made to adopt proposed standard 8A:

8A. Access to the “Customer Activities” site should be protected by HTTP Basic Authentication or similar logon/password mechanism(s) using 40-bit SSL. A “Customer Activities” site should typically require a single logon/password pair for each user session.
VOTE: The motion passed unanimously as a recommended standard (4.3.x).
As a note to the EII task force, the FTTF noted visibility options: Provide a link to the “Customer Activities” site from the “Informational Postings” site.

[2] FTTF noted that the cost of implementing these private network connections is recognized as an
issue but was determined to be out of the scope of FTTF.

Provide a link to the “Customer Activities” site from the “Informational Postings” site at the option of the TSP.
Provide a link to the “Customer Activities” site from the “Informational Postings” site only after a user has been authenticated into the “Customer Activities” site.
Do not allow a link to the “Customer Activities” site from the “Informational Postings” site.
Discussion on risks of displaying link to “Customer Activities” site: It has been suggested that the “Informational Postings” site include a link to the “Customer Activities” site. Additionally, a link to the “Informational Postings” site would be included in the menu of the “Customer Activities” site. These reciprocal links would add a natural navigation between the transactional and non-transactional areas of a site provider. Thus, a user who is working on a transaction would easily be able to transition to viewing a posting or other content provided in the non-transactional area or site. This transition is without question a good idea and poses no technical risk.
The converse link, showing the “Customer Activities” link on the “'Informational Postings” is the one that raises concern. If the link to “Customer Activities” is displayed on a public site (which the Informational Postings site is) there is concern that it advertises the existence of a transactional system to hackers, vandals, or possibly parties wishing to attack the energy infrastructure from abroad. This concern focuses on the fact that the first step in attacking a site is to know that such a site exists. If this “Customer Activities” site is not visible as a link from the “Informational Postings” site, it would be possible to conceal the very existence of the transactional site. The argument that opposes this is that the risk in showing a site is not significant compared to the convenience provided in the reciprocal links described above. The technical ramifications of this debate are actually quite simple. The assertion that “a site that is not directly visible on a companies public sites is safer” is only partially true. For the “casual hacker” looking for an entry point to attack a company, this would likely be an effective first layer of security. For a concerted attack from skilled “hackers” or even countries, this would probably present little protection. Obviously, this could be argued at some length and neither type of event has been prevalent in our industry thus far. But the fact remains that a site not seen is safer to a degree.
Based on the security concerns mentioned above, EII should weigh the risks of showing the link against the convenience provided by the link.

The motion was made to adopt proposed standard 8B:
8B. At a minimum, data communications for the “Customer Activities” sites should utilize 40 bit encryption. Where possible, 128 bit encryption is strongly recommended.
VOTE: The motion passed unanimously as a recommended standard (4.3.x)

The motion was made to amend recommended standard 8A:
8A. Access to the “Customer Activities” site should be protected by HTTP Basic Authentication or similar logon/password mechanism(s) using 40-bit encryption. A “Customer Activities” site should typically require a single logon/password pair for each user session.
VOTE: The motion passed unanimously as a recommended standard (4.3.x).

The motion was made to adopt proposed standard 8C:
8C Custom downloadable modules presented by a “Customer Activities” site should be signed by the author. The signatures on these modules should be communicated in advance to site users.

VOTE: The motion passed unanimously as a recommended standard (4.3.x)

The motion was made to adopt the proposed implementation guide additional text:
Implementation Guide Content under Security for Customer Activities Sites:
THE LIST OF PRODUCTS BELOW REPRESENT A NON-COMPREHENSIVE SET WHICH A CLIENT MAY USE. THIS LIST IN NO WAY SHOULD BE CONSTRUED AS AN ENDORSEMENT BY GISB OF ANY SPECIFIC PRODUCTS. OTHER PRODUCTS MEETING THE MINIMUM TECHNICAL CHARACTERISTICS OF THE CLIENT WORKSTATION MAY BE USED.
(FTTF will review this on an annual basis during the version check cycle.)
Minimum
40 bit* SSL or 40 bit* RSA Java communications or 40 bit* Secure ICA
*128 bit encryption is strongly recommended where possible.
[THE ABOVE TEXT WILL BE REVIEWED FOR TRADEMARK, COPYRIGHT AND OTHER LEGAL CONSIDERATION PRIOR TO NOTICE FOR INDUSTRY COMMENT.] SPECIFIC PRODUCTS SHOULD BE REVIEWED PRIOR TO IMPLEMENTATION FOR YEAR 2000 COMPLIANCE.
VOTE: The motion passed unanimously as an addition to the implementation guide.

The FTTF noted that although non-repudiation is a very important feature, it is impractical to implement on the “Customer Activities” Web sites using currently available non-proprietary technology. GISB should continue to evaluate potential tools, and create standards and guidelines for its implementation as soon as the technology will support it. FTTF will review this on an annual basis during the version check cycle.

The FTTF noted that although the Camel Model specifies that client-side certificates should not be required; they may prove necessary for non-repudiation. Topics such as certificate authorities remain to be researched. GISB should not require client-side certificates at this time, but will probably be necessary in the future. FTTF will review this on an annual basis during the version check cycle.

The motion was made to adopt the proposed standard forwarded by Duke Energy:
8D In the Navigational Area of the Informational Postings Web Site, the navigational link for "Customer Activities" should appear directly above the navigational link for "Site Map."
VOTE: The motion passed as a recommended standard through the following vote:
Segment For Balanced For Against Balanced Against
End User 1 1 0 0
LDCs 1 1 0 0
Services 7 1.75 1 0.25
Producers 2 2 0 0
Pipelines 16 1.68 3 0.32
TOTAL 27 7.43 4 0.57

The motion was made to adopt revised proposed standard 9A:
9A. Private network connections to GISB EDM* sites may be at any point on the TSP firewall boundary at the TSP's discretion on a non-discriminatory access basis. The specific type and speed of these connections should be mutually agreed. It is at the discretion of the TSPs on how multiple private network connections should be managed, so long as such management is done on a non-discriminatory access basis. TSPs are not responsible for any additional security exposures when using these private network connections.
* This includes all GISB standardized Internet communication.
VOTE: The motion passed unanimously as a recommended standard (4.3.x).

The motion was made to adopt proposed principle 10A:

10A. Trading partners should maintain redundant connections to the public Internet for GISB EDM* sites. These redundant connections should be topographically diverse (duality of) paths to minimize the probability of a single point of failure.
* This includes all GISB standardized Internet communication.
VOTE: The motion passed unanimously as a recommended principle (4.1.x).

The motion was made to adopt the following text for the Implementation Guide Content under Redundancy:
Implementation Guidelines for Redundancy*
*In this context redundancy refers to normal operations redundancy (as opposed to disaster recovery contingencies).
Customer Activities Sites
Users and providers should consider but not be limited to the following possibilities to achieve redundant connectivity:
1 Multiple dial-up connections
2 Multiple leased line connections
3 Multiple Internet service providers
4 Combinations of the above
5 Geographically diverse connections
6 Topographically diverse connections; i.e., connections which result in Internet pathways that do not pass through a single point/service/router
7 Multiple power sources for network equipment Items 1-5 are potential means of achieving the defining characteristic of item 6. The intent is to eliminate the possibility of a single point of failure.
EDI/EDM Sites

Three possible approaches are:
1 Maintain multiple ISPs and multiple points of connectivity, each of which was identified by the same URL making the process of redundancy transparent to the sender.
2 Maintain different Internet connectivity URLs (presumably on topographically different ISPs). For this to result in communication redundancy, the sender should know of the existence of the secondary URL and have programming in place that will automatically switch batch-browser transmissions to the secondary URL when the primary URL is unavailable.
3 Maintain multiple connections to the same ISP. This involves only one URL but the presumption would be that the ISP would provide alternate diverse paths for the URL.
Receivers may maintain multiple URLs and, if such have been disclosed, the sender should attempt to use these during primary URL outages. The redundant public Internet connections can be through a single ISP or multiple ISPs.
If multiple URLs are provided for EDM access, the following conditions should be met:
The information provided by each URL should be exactly the same, although trans-ids can be different.
The trading partners should be informed of both URLs and their availability by system wide notice or by TPA.
The URLs should be identified as primary and secondary if either:
There is a TSP connection speed difference between the URLs (The faster connection listed as primary).
or
One URL is only available when the other is down (primary URL being the most available).
The URLs should be listed as primary and alternate if:
The URLs have the same TSP connection speed.
and
The URLs are customarily available simultaneously.
Note: A URL is considered available (in the context of communication redundancy) if all the IP facilities are properly functioning up to and including the HTTP service. This would include any TSP provided facilities including firewalls, DNS servers, routers, hubs, LANs, etc. that are between the TSP's HTTP server and the ISP's point of presence.

VOTE: The motion on the addition to the implementation guides for guidelines for redundancy on Customer Activities sites passed unanimously.

Items from October 1/2, 1998 EII Meeting

- Recommend to FTTF that they review the recommendation of 800 x 600 display resolution.

Items from November 2/3/4, 1998 EII Meeting

- **III. Future Technology Task Force Recommendations**
  Ms. Croley reviewed the proposed standards for Client Firewall Requirements for Service Provider EDM Implementations:
  76 Principle:
  Transportation Service Provider EDM implementations should minimize the number of outbound ports required to be opened on the client-side firewall.
  77 Standard:
  Transportation Service Providers should be limited to the GISB approved list of available TCP ports and UDP ports for EDM implementations included in the appendix in the Electronic Delivery Mechanism Related Standards manual under Client Firewall Requirements for Service Provider EDM Implementations.
  78 To be placed in the Electronic Delivery Mechanism Related Standards manual as implementation guidelines:
  Client Firewall Requirements for Service Provider EDM Implementations FTTF recommendations include the potential modifications needed in the client-side firewall to allow for communications with the various service providers' EDM implementations. The following is a list of allowable TCP ports available for use by a Service Provider. Upon request, the Transportation Service Provider (TSP) should indicate to their trading partners which specific ports they will require to be opened to conduct electronic communication.
  Allowable TCP Ports (not UDP ports):
  HTTP 80, 5713, 6112, 6304, 8674, 7403
  SSL 443
  ICA 1494
  RMI(Java) 1099-1100
  Java Telnet 31415
  TCP Optional 8001-8020**
  Allowable UDP Ports (not TCP ports):
  Secure ICA 1604
  There are other technologies available that will require additional ports to be opened, such as FTP, Telnet, and SMTP. If and when GISB approves such technologies, FTTF will modify this list of allowable ports accordingly.
  The client-side firewall implementation and client browser settings should permit the downloading and installation of GISB approved plug-ins and modules. Please refer to the GISB defined Minimum Technical Characteristics for Accessing Customer Activities Web Sites for the listing of plug-ins and modules.
  These guidelines will be reviewed and updated by the Future Technology Task Force, at a minimum, by the spring of each year and presented to the GISB Executive Committee for adoption by the June meeting of that group.
  ** The reservation of 20 optional ports was to provide room for implementations such as DCE, IIOP, and load balancing implementations. TSPs should endeavor to minimize the usage of these ports.
  Ms. Scott asked that the following proposed standard also be considered, and amendments were made:
  79. Standard
  TSP EDM implementations should not require any inbound ports to be opened on the client-side firewall.

Vote: The above standards (item nos. 77 and 79), principle (item no. 76) and implementation guide text (item no. 78) were adopted unanimously.

Ms. Croley reviewed the proposed standards from the Future Technology Task Force regarding the Flat File/EDM model, both for batch processing and interactive processing. She recommended two definitions (item nos. 80 and 81), two new standards (item nos. 82 and 83) and a change to existing EII recommendation (recommended standard S34) for security, one new standard for protocol (item no. 84), and three clean-up items (GISB Standard Nos. 4.3.8, 4.3.2 and 4.3.9). Further changes may be needed to other standards as outlined in the Future Technology Task Force work paper and Ms. Van Pelt, Mr. Tsucalas and Ms. Croley will work on suggestions to the GISB standards language off-line. The proposed standards from the Future Technology Task Force are:
80. Definition
"Batch Flat File" is the term used within GISB FF/EDM to describe the automated computer to computer transfer of flat files.
81. Definition
"Interactive Flat File" is the term used within GISB FF/EDM to describe the transfer of flat files using an interactive browser.
82. Standard
For Interactive Flat File EDM, 40-bit Secure Sockets Layer (SSL) encryption should be used. Where possible, 128-bit SSL encryption is strongly recommended.
83. Standard
For Interactive Flat File EDM, access should be protected by HTTP Basic Authentication.
S34 Revised Recommended Standard:
In the course of our review of potential conflicts with existing EII standards on security with what we would consider for Interactive Flat File EDM, we recommend that EII Standard S34 be changed to remove the words "using 40-bit encryption", so that the revised standard would read: "Access to the customer Activities Web Site should be protected by HTTP Basic Authentication or similar logon/password mechanism(s). A Customer Activities Web site should typically require a single logon/password pair for each user session."
4.3.8 Revised GISB Standard:
Correct standard 4.3.8 to insert the word "be" before the word "HTTP" in the first sentence, so that the revised standard would read: "The minimum acceptable protocol should be HTTP. All sending and receiving parties should be capable of sending and receiving using HTTP."
4.3.2 Revised GISB Standard:
Correct standard 4.3.2 to replace the word "designed" with "designated", so that the revised standard would read: "On time stamping, data leaves control of the originator by the same time (deadline), regardless of mechanism (3rd party service provider time stamp is acceptable) and 15 minutes of communication time should be available to allow accumulation of all transactions to the pipeline. A standard network protocol (TCP/IP) should be in service for direct connect to the pipeline designated site by 4/1/97.".
4.3.9 Revised GISB Standard:
Lead the standard with the phrase with "For EDI/EDM and FF/EDM, ...", so that the revised standard would read: "For EDI/EDM and FF/EDM, there is a time stamp (HTTP Time-stamp) that designates the time that a file is received at the designated site. The receiving party should generate a time-stamp upon successful receipt of the complete file and send as an immediate response to the sending party. The time-stamp should be generated by the Common Gateway Interface (CGI) of the receiving party, prior to further processing by the CGI.".
Vote: The above standards (item nos. 82 and 83), definitions (item nos. 80 and 81) and revisions (item no. S34, GISB Standard Nos. 4.3.8, 4.3.2 and 4.3.9) were adopted unanimously.

Ms. Croley then requested that the following clean-up item be addressed:
D4 Revised Recommended Definition:
Eliminate the phrase 'computer-to-computer" so that the revised recommended definition would read" "'GISB FF/EDM' is the term used to describe a standardized flat file electronic data interchange of information in files as mapped from the x.4.z GISB standards. GISB FF/EDM is

communicated between trading partners over the Internet using the GISB Electronic Delivery Mechanism."
Vote: The above revision to recommended definition D4 was adopted unanimously.

Items from November 2/3/4, 1998 EII Meeting

- R99022 The following motion was made:
  Instruct IR and FTTF to define a means of sending a Capacity release dataset which will allow the replacement shippers to electronically execute the contract for the awarded capacity. Incorporated into this function is the need to be able to determine the specific user who is submitting the electronic execution to ensure that they have been identified as being authorized to perform this function.
  Action: Request R99022 was deferred for review until contracts are discussed.