MEMORANDUM

TO: Chairs of the EBB Internet Implementation Task Force - Carl Caldwell, Mike Novak, Tammy Hopkins, Dona Gussow, Paul Keeler

FROM: Susan Croley, Chair of the Future Technology Task Force

SUBJECT: REPORT ON RECOMMENDATIONS TO THE EBB INTERNET IMPLEMENTATION TASK FORCE

DATE: September 11, 1998

CC: Rae McQuade, Mike Bray, Jerry Hahn

In the attached document, are the standards, implementation guidelines, and notes to the EBB Internet Implementation Task Force (EII) that the Future Technology Task Force (FTTF) has developed thus far in response to the tasks delegated to FTTF by EII through the Camel Model and other EII directives. FTTF will present a report on their recommendations to EII at the September 17, 1998 meeting in Arlington, Virginia.

Directive Topics - **Minimum Technical Characteristics for accessing Customer Activities Sites; Standard Client Configuration**

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

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)

End of Implementation Guide Content

The motion on implementation guidelines on minimum technical requirements passed unanimously.

Note to EII:
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.

PROPOSED STANDARD
Providers of Customer Activities 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, 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 in the April meeting of that group.

This motion passed by 23, 0, 1.

Directive Topic **- Connections to Third Party Communication Networks**

PROPOSED STANDARD
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. TSPs are not responsible for any additional security exposures when using these private network connections.

*This includes all GISB standardized Internet communication.

This motion passed by 20, 0, 2.

Note to EII on Connections to Third Party Communication Networks:
For 18 /Abs: 3
Cost of implementing these private network connections is recognized as an issue but was determined to be out of the scope of FTTF.

End of Note to EII

Directive Topics - **Security; Site Visibility**

ACCESS
A. Authentication

PROPOSED STANDARD
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.

Note to EII on displaying the link to the Customer Activities Site:
B. Visibility Options

1. Provide a link to the "Customer Activities" site from the "Informational Postings" site.
2. Provide a link to the "Customer Activities" site from the "Informational Postings" site at the option of the TSP.
3. 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.
4. 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 as 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.

End of Note to EII

PRIVACY AND INTEGRITY

PROPOSED STANDARDS(2)
At a minimum, data communications for the "Customer Activities" sites should utilize 40 bit encryption. Where possible, 128 bit encryption is strongly recommended.

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.

Implementation Guide Content under Security for Customer Activities Sites:

(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.

End of Implementation Guide Content

NON-REPUDIATION

NO PROPOSED STANDARD
Note to EII:
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.

End of Note to EII

CLIENT-SIDE CERTIFICATES

NO PROPOSED STANDARD
Note to EII:
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.

End of Note to EII

Directive Topic - **Redundancy**

PROPOSED STANDARD
Trading partners should maintain redundant connections to the public Internet for both EDM and Customer Activities Sites (CAS). These redundant connections should be topographically diverse (duality of) paths to minimize the probability of a single point of failure.

The motion for the standard passed 18, 2, 2.

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

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.

The motion on guidelines for redundancy on Customer Activities sites passed unanimously.

EDM Sites (Batch)

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.

End of Implementation Guide Content

Motion passed unanimously to accept the implementation guidelines drafted on redundancy for EDM (Batch) sites.