Workpaper
GISB EDM Subcommittee Response to Sandia National Labs Report

EDM Types from GISB EDM Manual	Applicable Encryption Standards	Sandia Recommendation	Terry's Recommendation
1. EDI & Batch Flat File	4.3.15	Secure (7.1.5)	Secure using 128-bit encryption
2. Informational Postings	4.3.20	Secure (7.1.6)	Non-Secure—present intercept/alter issue to BPS
3. EBB (Customer Activities)	4.3.60, 4.3.61	Secure (7.1.6, 7.1.7)	Secure using 128-bit encryption but no digital signature
4. Interactive Flat File	4.3.83, 4.3.84	Secure (7.1.6, 7.1.7)	Secure using 128-bit encryption but no digital signature
	CAR—4.3.20	CAR—Secure (7.1.4)	CAR—Non-secure—present blocking legitimate users issue to BPS

So what do we need to do?

1. We need to develop a GISB Standard for EDI & Batch FF security. Presumably, this standard would require the use of 128-bit security.
2. We need to discuss the pros and cons of developing a GISB Standard for Informational Postings security, indicating why security is not needed.
3. We need strengthen GISB Standard 4.3.61 to require 128-bit security for EBB (Customer Activities) EDM.
4. We need to strengthen GISB Standard 4.3.83 to require 128-bit security for Interactive Flat File EDM.
5. We need to address security requirements for the Central Address Repository (which is a data type rather than an EDM type) in order to provide a response to Sandia's item 7.1.4.

Existing GISB Standards on Encryption:

4.3.15 Trading partners should implement all security features (secure authentication, integrity, privacy, and non-repudiation) using a file-based approach via a commercially available implementation of PGP 2.6 or greater (or compatible with PGP 2.6). Trading partners should also implement basic authentication. This should be regarded as an interim solution since this technology is not an open standard. This technology supports all of the above security features while providing independence of choice of Web servers and browsers. Encryption keys should be self-certified and the means of exchange should be specified in the trading partner agreement.

4.3.20 A user ID or password should not be required to access the Central Address Repository or the TSP's Informational Postings Web Site.

4.3.60 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.

4.3.61 At a minimum, data communications for Customer Activities Web sites should utilize 40-bit encryption. Where possible, 128-bit encryption is strongly recommended.

4.3.83 For Interactive Flat File EDM, 40-bit Secure Sockets Layer (SSL) encryption should be used. Where possible, 128-bit SSL encryption is strongly recommended.

4.3.84 Access to Interactive Flat File EDM should be protected by HTTP Basic Authentication.

Using the above for reference, here are my inputs:

1. We should address 5 types of data/ access as suggested by the table above. For clarification, these are:
    a. EDI & Batch Flat File
    b. Informational Postings
    c. EBB/ Customer Activities
    d. Interactive Flat File
    e. Central Address Repository (CAR)
2. Suggestions/ comments for each (see corresponding letter in item 1 above) follows:
    a. EDI & Batch Flat File – Sandia recommends that we encrypt the HTTP message to ensure that the user id and password are encrypted. Discussion at the 2-14-2001 meeting yielded general agreement that we should take Sandia's recommendation. We also agreed that this should be accomplished using Secure Sockets Layer (SSL) with 128-bit encryption. It is believed that programming libraries exist for all platforms to accomplish this in the batch browser software. It is also believed that all Web servers are capable of this. The batch browser and the Web server are the two software components used to exchange X12 and Flat Files in the current GISB standard. Those in the meeting were to follow-up with their technical teams to confirm this in their companies. We will rely on any feedback from the greater GISB membership when our recommendations are made available for comment to have confidence that this will work for all.
    b. Informational Postings – Sandia's report does not seem to distinguish Informational Postings from Customer Activities. They simply refer to "Interactive Processing" and "transactions". Participants in the 2-14-2001 meeting agreed that we should distinguish between Informational Postings and Customer Activities in our response to Sandia's report. We also agreed that Informational Postings have always been considered information available to the public at large. Therefore, GISB standards have intentionally not imposed any security requirements for this data category. Since this information is intended for the public, an authentication mechanism (such as a logon) should not be imposed. By not encrypting this data, we are vulnerable to someone intercepting the message and altering its content prior to it being viewed by the requestor. This requires a fair amount of effort to accomplish. This possibility should be presented to the "Business Practices" committee for their consideration and feedback. We could apply SSL encryption to this content to prevent this possibility but it should noted that this will have a slight adverse affect on response time. Digitally signing this "display only" content, if possible, would have no value as the Web browser has no mechanism to utilize the attached signature.
    c. Customer Activities – As noted in Sandia's report, GISB standards already call for applying encryption to Customer Activities data. However, the current standard makes 128-bit encryption optional. Discussion in the 2-

14-2001 meeting favored making 128-bit encryption standard. However, Sandia also suggests applying a digital signature to this data. A digital signature provides for non-repudiation. This means that the source of the transaction is provable and tamper-proof. They suggest using PGP with its ability to digitally sign what is on the clipboard. It is acknowledged that Sandia's recommendation suggests the best-known way to deliver non-repudiation. This would require that the browser contain code to write and read content to and from the clipboard. This appears to be supported with the most recent versions of IE and Navigator. It should be noted, however, that the user could disable pasting via script in IE (not sure about Navigator). However, our current standard allows use of the ICA protocol (AKA Windows Terminal Server). This protocol moves screen images to the client but the data entry form is actually running on the server machine, not the client. In this case, there is no way for the user on the client side to apply a digital signature using its private key. (It is likely that Sandia was unaware of the implication of using this protocol). Using PGP creates a considerable administrative burden as well since the trading partners (especially, TSPs) would have to maintain, in many cases, a very large number of public keys. PGP keys are often exchanged using diskettes and the US Mail since use of email can be an insecure key exchange mechanism. There may be performance issues as the size of the PGP key ring grows to be very large. As we are also considering an expiration period for these keys, the administrative task may grow even more. Of course, use of PGP by every on-line user means that they must purchase the PGP software and it must run on their desktop. This may affect sites that attempt to achieve a standard configuration and minimal client-side software for their users. Additionally, it creates a training requirement for the users. All in all, this approach appears to be unfeasible (especially due to the ICA problem). Another alternative is the possibility that the browsers provide for signing of Web forms using a certificate. A check with Microsoft revealed that even IE 5.5 does not have this capability which means this alternative is not available since it must work on both IE and Navigator (did not investigate Navigator as the point is moot). It appears that we will be unable to provide for non-repudiation by applying a digital signature to an interactive transaction. Disallowing the ICA protocol may make this more possible but it is still burdensome, at best, to implement this feature. It is suggested that we forego this until such time as a more practical approach is possible.

d. Interactive Flat File – The Interactive Flat File mechanism allows the user to construct a comma-separated-value (CSV) file using software such as a spreadsheet and then upload it using a Web browser. It makes sense to utilize 128-bit SSL encryption to protect this data from viewing or alteration. Because the uploaded transaction is in the form of a file, it is possible for the user to apply a digital signature to the file after its creation. The same administrative issues as described in 2c above apply here. That is, there is the potential to have to maintain a large number of

PGP public keys. However, as a practical matter, there appear to be very few users of this particular EDM mechanism, which reduces the administrative burden. Of course, the user would still be required to purchase and install the PGP client on the desktop and there would still be a training requirement. However, there appears to be little to be gained by having this capability for this particular on-line user while most on-line users would not have the capability. For this reason, it suggested that we implement 128-bit SSL encryption but forego implementing digital signature for this type of EDM.

e. Central Address Repository (CAR) - Sandia suggests that we protect the CAR using both SSL encryption and a logon authentication. As the CAR data is read-only, this imposes a requirement only on GISB's Web site. It is relatively easy to implement, especially if there is only one userid and password to be used by all GISB members. The GISB office, via a mailing or the annual meeting, could provide this information. The only question is whether this would have the effect of unintentionally blocking access for legitimate users. This question should be addressed by GISB.