

GISB EDM Subcommittee

03/13/01

Sandia Action Plan - Proposed Responses

Sandia Item 7.1.12 - Message Replay Attacks

Sandia Concern: GISB EDM may be susceptible to replay attacks by a third party intercepting a message and replaying it repeatedly to destination server - a "deep denial of service" attack.

GISB Response: The adoption by GISB of SSL encryption for EDM messages (see item 7.1.5) precludes the interception of the message by a third party for replay. While this technique does not preclude the possibility of a replay attack from a "man-in-the-middle" (DNS spoofing), it does mitigate the most likely causes of replay attacks.

Sandia Item 7.4.5 - GISB EDM Document Compatibility

Sandia Concern: Version compatibility is not discussed in the GISB standards or the TPA. Suggested revising TPA and including statements about backward compatibility.

GISB Response: Proposed GISB Principle 4.1.X

"Trading Partners should mutually select and maintain a version of the GISB EDM standards under which to operate."

Sandia Item 7.2.1 - Grouping of Principles

Sandia Concern: Principles should be (re)organized by topic, instead of chronologically.

GISB Response: While GISB recognizes the chronologically organization of the Principles may appear arbitrary to the unknowing reader, the organization of Tab 4 is consistent with the organization of all GISB standards.