



Analysis of Sandia Surety Report on GISB EDM

Dick Brooks

CTO, Group 8760

GISB EDM Committee

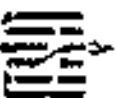
co-Chair

General Observations

- Report is generally positive
- EDM is a good foundation for GISB's needs
- Sandia recommendations to address weaknesses are technically feasible within EDM
- GISB EDM v1.5 addresses some weaknesses identified by Sandia

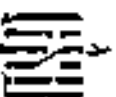
Sandia Recommendations

- Areas Impacted
 - Documentation
 - Standards
 - Principles
 - TPA
 - EDM Specification
 - GISB EDM Protocol
 - Batch Browsers
 - EDM Servers
 - Web Servers



EDM Protocol Weaknesses

- Some Transactions Unauthenticated
 - Error Notifications
 - Timestamps
- Some Data Not Kept Confidential
 - Error Notifications
 - Timestamps
 - Username/Passwords
- Message Replay Allowed



Possible Solutions

- Some Transactions Unauthenticated
 - Addressed in GISB EDM V1.5
 - Optional support for digitally signed error notifications and timestamps
 - NO additional changes needed to EDM V1.5



Possible Solutions

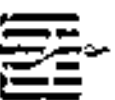
- Some Data Not Kept Confidential
 - Use 128 bit SSL sessions to encrypt all data
 - IETF EDIINT AS2 currently supports SSL via TLS (RFC 2246)
 - Web Servers already support SSL
 - Requires changes to Batch Browser software
 - Impacts data transfer performance
 - NOT currently addressed in EDM V1.5 specification

Possible Solutions

- Message Replay Allowed
 - Addressed by requiring digital signatures and unique message identifiers on all messages
 - Would require changes to EDM v1.5 impacting both batch browsers and EDM servers

Summary

- Weaknesses identified by Sandia can be addressed with existing technology
- Some weaknesses are already being addressed in EDM 1.5
- Open issues could be addressed in EDM 1.5 with relatively minor enhancements (mainly by requiring SSL and unique message identifiers)
- Significant portion of the proposed changes affect GISB specifications



Questions

