**Webinar Minutes**

**OpenSG SG Security Cybersec - Interop Task Force Review Subgroup**

**Syslog Proposal Review**
**Tuesday, Aug 24th at 1:00 – 3:30 PM Eastern**

Attendees:

| | |
|---|---|
| Pete Capani | Oncor |
| JD Senger | Oncor IT security manager |
| Dominic Iadonisi, | Ruggedcom |
| John Stewart | TVA |
| John Lilley | SDGE security |
| Gerald Paprocki | Elster, software design manager |
| Sandy Basik | Enernex, principal consultant |
| Adrian Mclenahan | Data Track |
| Joe McCormick | Data Track |

**1. Introductions and Background**

Value of standardized syslog to the Smart Grid

---------------------------------------------

McCormick: Standard syslog essential to system of system troubleshooting in a multivendor environment. Allows for syslog evaluation automation.

Iadonisi: Learning from SNMP evolution. Public versus private MIBs. Public MIB similar to standard syslog records.

Paprocki: Historicaly, CEE, CEF standards attempted for standardizing log formats. Leverage those efforts.

The following URL's were furnished by Gerald Paprocki

A link to the CEE Common Event Expression web site is as follows:
http://cee.mitre.org/

You can also check out section 5 which provides a history of several of the log standardization efforts.
http://cee.mitre.org/docs/Common_Event_Expression_White_Paper_June_2008.pdf

Stewart: Keep focus on limited level, don't get scope too far out.

JD Senger: NISTIR 7628 references old syslog RFC (3164) for Advanced Metering System support. Rev 2 of the NISTIR is coming out. Also NIST SP800-92 mentions RFC 3164.

Teumim: Going through proposal. Need to check NISTIR, etc and talk with writers (Jim Gilsinn of NIST may be the writer of that section)

McCormick: I don't see anything from 3164 coming back from latest searches of the 3 sections of the draft of the NISTIR.

McCormick: Don't forget there needs to be a time server to sync time, probably NTP.

Lilley: 5424 should be backward compatible with 3164.

**Subgroup member conclusions:** on the 3 item proposal at end of document, on proceeding with plan for standardizing 3164, adding to freetext area in 3164 for extra (NERC-CIP ? ) info, use of 5424 for next generation Smart Grid.

Data Track and Ruggedcom: that rewriting to the proposed standard scheme in 3164 would be acceptable, provided it is timed with an engineering release

Elster: not ready with feedback yet.

End-User input:

Pete Capani: Proposed scheme acceptable

John Stewart: Yes, push for standardization as in proposed scheme

John Lilley: Was in favor of starting with newer (5124) format, not spending time on old format.

Discussion: Backward compatibility between standards. Use newer standard in aggregators, deal with older messages from existing devices. Where to start? Phased approach as in draft? Focus on content rather than structure? Defining initial, common, preferred keyword/value pairs to get started?

It was determined that Microsoft Server 2000, 2003, and 2008 used RFC 3164. Server 2008 also uses 3195 extensions.

Teumim: Table 1 can be used to start the common terms/pairs. Intermediate step: 3164-compatible device, put UTC stamp in free text at end of record. And any other info necessary put at end of record beyond that UTC stamp.

Summing up

==========

Teumim: Table 1 can be used to start the common terms/pairs. Intermediate step: 3164-compatible device, put UTC stamp in free text at end of record. And any other info necessary put at end of record beyond that UTC stamp.

### Summing up

Majority on call agree that Lemnos proposal per circulated document is a good way to proceed.

Reminder to look at other standard log message efforts and note if they were successful

Phased schedule to modify 3164 structure to 5424 where more flexibility exists. Industry not ready

for 5424 at the moment

### Action Items

Teumim: Put out 30 to 40 standard messages. Give an example of 3164 with added detail for NERC in the free text field.

Teumim: Look at NISTIR for mention of 3164 vs 5424

Talk to Dave Dalva . He co-chaired NISTIR 7628 group.