

MTLG

13-Mar-201

update 5070bis draft title with MTLG

## SCI

MTI decision - choose IEEE MMDF as the mandatory to implement part of the spec

Missing items before WGAC:

Eric Burger - MTI is always good but it isn't an IEEE document; so it may not be stable

Sean Turner - will work through IEEE liaison to determine status

Eric - can allow non-normative ref

Sean - non-normative okay; it's fine now

Hum - many in favor; no opposed

## 5070bis

Paul Hoffman - section 1.1 doesn't match the addition boxes on the slides  
(DOS, Win-Reg keys, files, mail headers, HTTP headers)

MILF

## 5070bis

Question which things should be added? which things are too complicated and should be extensions

Paul Hoffman - win Reg keys - too complicated to include

Murray - interested in possibly having additions for SMS abuse. doesn't really care about if its in IODEF or extensions

Paul Hoffman - caller ID abuse

should core things be things under FETF; everything else as an extension?

Kathleen - line maybe possibly is things that are commonly shared

Hoffman - not commonly shared? maybe better is "things we know how to share"

Murray - maybe extension can be done simultaneously w/ 5070bis

~~Chris~~ - SMS should be handled

Dave Waltermire - what are the use cases, articulate them?

MILE

Roman - 2 co-mingled use cases

Sean Turner - Use Cases should go in charter

Q: how do enumerations / extensions work?  
Brian - is there an XML tech for this? rdd-didn't find it  
Dave Watterline - doesn't know of one

Paul Hoffman - problem with enumerations

Chenry Adams - RFC 3333

Indicator Set Id / Indicator UID -

D Watterline - why do you need sets?

Paul Fiedler -

D Watterline - what about logical set operations OR's & AND's

RDD - it's across documents

Domain -

~~Rather~~ - RFC 5901 class has most of data  
Should the Schema be changed / pulled out

RDD - should it be in CORE or not

Paul Hoffman - tomorrow in DNS proposal to export DNS responses as JSON

Danny (?) - NMSG is also in use  
to exchange DNS

Brian Trammel - backporting international  
changes from R100

Owe ~~Black~~ - backporting probably won't work

Sean Turner - let the experts deal w/  
internationalization standards

Other issues -

Eric Berger - version issue

Draft has a lot of SHOULDs;  
need to define reasons when using a  
SHOULD when not to define it

Sean Turner - agree w/ SHOULD

Paul Hoffman - should have some should  
questions

SHOULD people - Eric Berger &

Sean Turner - be able to remove stuff

Paul Hoffman - any enum change breaks  
backward compat

Sean Turner - the cool kids use JSON

## MILE

Paul Hoffman - JSON has no validity checkers

Sean Turner - timeline of updates vs.  
JSON validator

C. Henry Adams - Should include SMS

Murray - enough people interested in  
sms & JSON that they would work  
on validator

Chair - Wes Young w/ CIF has done a  
conversion from XML to JSON

B+T - whined like a little girl over  
draft naming

## ENUM Ref Format

Dave Black - will help w/ IANA considerations

Eric Burger - should use XML for XML; to  
validate fields

need lots of additional text to  
spec handling of all sorts of  
degenerate strings

Dave Black - this is a 5070 fix not  
5070 bis? otherwise tweak XML

- Eric Burger - as 5070 fix okay; otherwise ...

MILE

Chair - do we need ENOM before  
5070bis comes out?

<no answer>

C. Henry Adams -

Paul Hoffman - might be worth doing this  
work to learn the lessons by doing  
this

ROLIE

Paul Hoffman - mandatory auth??  
information sharing - likely need auth  
information access - maybe not so likely

Dave Wetherire - clarifying - want implementations  
to support having strong auth; not  
requiring strong auth always

Paul ?? - if you share info who  
do you trust about reputation; serious  
scope creep

(M)ARF

~~Paul~~ Murray - Includes the entire email  
message in ARF; so a lot of  
unpacking

what makes sense

## MIME

Pierre St. Andre - maybe can explain it

~~Ped~~ Murray

- currently all about email  
includes headers, time, etc.  
fields: data  
format

contains 3 mime sections, including  
entire email msg

C Henry Adams - ARF needs to be considered  
but refined

Pierre St. Andre - email community sticking  
w/ ARF

~~Ped~~ Murray

- mail community not looking to  
move from ARF; but willing  
contribute back /

Dave Walterire - ARF designed for SMTP  
transport?

~~Ped~~ Murray

- it's MIME, so yes but it can  
be over many transports

Dave - so are we interested in  
many transports

Chair - interested in many transports  
I workflows supported

## MILE

~~Paul~~

Murray - email community close to security, especial for spear phishing and exchange is likely more workable w/ IODEF wrapping ARF

(reign)

- communities are probably closer then they seem should figure out pivot points in the data

## Charter

Line to draw for 5070bis inclusions

Enum reference work seems good

Rollie to 5070bis alignments

5070bis is good

John Fidd - agree Rollie needs to capture those updates

Sean Turner - Draft charter on list by next Friday

Kent Handford - Changing model from incident sharing to indicator sharing

Paul Hoffman - not change, but in addition