Proposed email in the thread “Re: Cooperation with the strategy project” specifically to Chet’s Message last week on the 19th

Greetings Everyone,

There are a few items I want to address regarding the possible use of the Emergency Data Exchange Language Situation Reporting (EDXL-SitRep) Version 1.0 Committee Specification 02 dated from 06 October 2016, [available here](http://docs.oasis-open.org/emergency/edxl-sitrep/v1.0/cs02/).

First, this specification is extensible using edxl-ext-v1.0.xsd contained in the zip package of all formats of the specification document, and all required schema for edxl-sitrep-v1.0. So it is possible to implement additions to the specification if or as needed.

Second, there are five pre-defined report messages in edxl-sirep-v1.0:

**FieldObservation Report Type**

**SituationInformation Report Type**

**ResponseResourcesTotals Report Type**

**CasualtyAndIllnessSummary Report Type**

**ManagementReportingSummary Report Type**

I would advise that looking into these specified report types to see if there are already terms/datatypes that can assure accurate data exchange. Specifically, critical infrastructure is included in/referred to in the data dictionary in the element **damageAssessmentInformation**.

However, this is the only mention of critical infrastructure, so it may well be that more is needed.

Knowing this I searched on the definition used in the [EU documentation](https://ec.europa.eu/home-affairs/pages/page/critical-infrastructure_en) and found:

Critical Infrastructure is an asset or system which is essential for the maintenance of vital societal functions. The damage to a critical infrastructure, its destruction or disruption by natural disasters, terrorism, criminal activity or malicious behaviour, may have a significant negative impact for the security of the EU and the well-being of its citizens.

The EU also defines Critical Information Infrastructure:

52009DC0149

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection - "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" {SEC(2009) 399} {SEC(2009) 400} /\* COM/2009/0149 final \*/

The US does not define Critical Information Infrastructure.

The US defines [Critical Infrastructure](https://csrc.nist.gov):

System and assets, **whether physical or virtual**, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

Since there is this difference, it might be wise to solicit the participation of OASIS Cyber Threat Intelligence Technical Committee (CTI TC) mentioned in this thread.

Third: Given the second item above, I think we should be very certain and specific defining exactly what we mean by Critical Infrastructure.

Regards,

Rex Brooks