Hi,

My name is Scott Pinkerton – I work at Argonne National Laboratory, and have been operating a near real-time cyber threat data exchange within DOE since 2004. [Would be happy to talk further if you wanted.]

I've included the following items that we feel are important in an information sharing framework:

* Near real-time (we operate today at 300 seconds, with plans to go fast)
* Autonomic; machine-machine transfer (not to rely on interactive portal-style data scraping)
* Payload agnostic – need to allow the transfer of numerous different file formats (E.g. STIX, IODEF, OpenIOC, CSV, IDS signatures, "reports", etc)
* We use an "envelope" with the various payload messages – place to store appropriate meta-data, especially when the payload doesn't naturally include.
* All data/info being shared needs to explicitly include the identification of who the data is being shared with; goes without saying that all-in/peer-peer sharing frameworks are not good enough
* Needs to be simple to share data with many (E.g. All of DOE, or all of civilian .gov) or with just one organization/site.
* Easily extensible – add new payloads (data types/formats being shared)
* Easily extensible – to add new participants both individual and "sectors"
* Flexible – needs to easily allow people to share data with large organizations (all of DOE, or all of *.gov) or by CIKR reference – energy sector.
* Flexible – needs to easily allow include or exclude of organizations or sites from the default sharing list
* Needs a simple interface – we use a client server model.
* Shouldn't required complicated FW rules (permission models) from the typical client
* Shouldn't use constantly open/active communication protocols
* Needs to easily integrate into an organizations (sites) work-flow (including integration into perimeter protection tools like FW, IDS's, e-mail filters, DNS systems, etc)
* Needs to support levels of obfuscation – different than anonymization. When we share cyber threat data within DOE – we see the internal attribution. ANL would know that this piece of threat data came from ORNL. However, when that same data was passed on to US-CERT the attribution would be modified to generically say it came from DOE rather than coming from ORNL. Control the first phone calls if someone at US-CERT wants to follow up on the information.

Anyway, just a quick dump from the top of my head.

-scott