Security Contact Metadata Extension

This content has been moved to Security Contact Metadata Extension Schema and may no longer be accurate

As part of the work for phase 1 of the SIRTFI implementation plan (https://wiki.refeds.org/display/GROUPS/SIRTFI), SIRTFI is proposing a security contact metadata extension, with the intent that it would be adopted by REFEDS member federations in order to allow handling of security incidents between federation partners.
InCommon has been using a similar metadata schema extension outlined below for several years and it has proven useful for IdP and SP operators. A recent presentation by Jim Basney at the WISE workshop gives more detail. The implementation within InCommon metadata is defined in this XSD, maintained by Ian Young: https://github.com/ukf/ukf-meta/blob/master/xml/incommon-metadata.xsd.

The proposed Sirtfi representation, including the revised REFEDS-namespaced URL for the contactType, is below:

Security Contact Metadata Extension

```
<EntityDescriptor ... >
...
<ContactPerson xmlns:icmd="http://refeds.org/metadata" contactType="other" icmd:contactType="http://refeds.org/metadata/contactType/security">
    <GivenName>Security Response Team</GivenName>
    <EmailAddress>mailto:security@institution.edu</EmailAddress>
  </ContactPerson>
...
</EntityDescriptor>
```

Who to expect there?

•Somebody in the entity organisation security team who knows about TLP and confidentiality
•Promptly (within one business day) acknowledge receipt of the security incident report.
•As soon as circumstances allow, investigate incident reports regarding resources, services, or identities for which they are responsible.
•Respond to the incident reporter and any other impacted parties when the incident is resolved.