Security Contact Metadata Extension Schema

Below is a security contact metadata extension for identity federations in order to allow handling of security incidents between federation partners.

Security Contact Metadata Extension

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

Who to include as the security contact?

- An appropriate security contact, such as an individual or generic contact, with existing security responsibility within an organisation.
- Existing incident response structures, including CERTs, may be leveraged where available
- This contact will:
    - Use and respect the Traffic Light Protocol (TLP) during all incident response correspondence
    - Promptly acknowledge receipt of a security incident report
    - As soon as circumstances allow, investigate incident reports regarding resources, services, or identities for which they are responsible

⚠ Correspondence sent to this address must not be publicly archived

Which fields must be provided?

GivenName and EmailAddress are mandatory for a Sirtfi security contact.

Can additional fields be included?

Additional information, such as telephone numbers or secondary email addresses, may be added if desired. Only fields from the OASIS Standard for contactType may be added.