Sirtfi WG google folder:

https://drive.google.com/drive/folders/13EhgPxzLy4U6FMP_cVDaIbqju40hOhUR

Current Task List

Who	What	When	Status
Nicole	FOs don't sign up for Sirtfi - create a template / criteria for involving them in incident response (i.e. get FOs to declare what they are doing and start actively monitoring this). Also encompasses defining what FOs should be doing during incidents.	In Progress	Raised at Steering Committee, small WG created.
Nicole	Peruse NGI Trust funded projects to identify any that may be relevant for Sirtfi.		
Christos	Propose a REFEDS 2020 Work plan item focused on understanding and potentially "regulating" proxy IdPs.		Closed
David G, Uros, **Sven**	Improve sharing procedures in AARC DNA3.2 paper by folding in experience from EGI.	Expected Dec 19, 2019	Delivered in FIR - Extending Sharing Procedures
Mario	Ask Dick Visser about taking control of sirtfi.org and CC Nicole		Asked, got answered this request was done
Tom	Agendize review of educational materials to see if we're done with that Phase 2 deliverable.		
Tom	See about TrustedCI assistance with an IR wiki	Jan 30, 2020	Shared feedback with WG on Jan 28, 2020
Uros, Tom	Provide initial considerations of establishing channels for incident response, and how can the communication be coordinated (considering edugain csirt)	Feb 13, 2020	To be discussed in the context of the eduGAIN support security team's IR communications workflow

March 12, 2020

Attending: Tom B, Mario Reale, Pål, Dave K, Alan B

Regrets: Uros, Hannah, David G, Laura P, Sven G

Agenda:

1. Marina and Romain report out on their discussion of:

   Talked a lot about ambiguity associated with the various roles addressed in these procedures. Does everyone involved in an IR know all of the others who have some role in it? Does everyone involved know how to directly or indirectly message others in their management of the incident? Marina and Romain will get together to address this before the next WG call.

2. Continue WG review and feedback on eduGAIN Security Incident Response Communication Workflow.
3. Compare/contrast ir_flowchart-1.pdf with the checklist at the bottom of eduGAIN Security Incident Response Communication Workflow. Pick one over the other, merge somehow, or another alternative?
4. Does the WG believe that the above sufficiently fulfill its deliverable of "Define incident response procedures for federations, including communication templates, and support the community in their adoption"?
   a. If so, how should we help prepare everyone to play their IR roles?
5. AOB

The group discussed the eduGAIN draft doc further and added some comments to it. In particular, should upward notification (to a fed op or to eduGAIN) always be given, or only if "necessary"? How should Sirtfi v2 address this? Should fed ops (eventually) be required by eduGAIN to have a "sufficient" IR Plan?

Proxies are like fed operators of a hub and spokes federation. They are also participants in a federation. It seems like they should play both roles under the eduGAIN doc. Yes? In particular, while an incident is only known to extend downstream from the proxy (contained within their own "federation"), should they bother to contact the federation of which they are a member?

More broadly, should notification about an incident be done only to manage the response, or is it also desired to notify upward (to fed op or to eduGAIN) for reporting or transparency purposes? This question is focused on the early stages of an incident - it is not about circulation of an after-action type of report.