Sirtfi WG google folder:

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

Current Task List

Who	What	When	Status
Romain	Gather IR plans from some e-infrastructures	Feb 6	
Mario	Brief Geant 4-3 IR meeting attendees on Laura's task, maybe arrange Laura's remote participation	Closed	I mentioned Laura's work to Daniel Kouril from GN4-3 - will need to include also others in the loop. Will get back to Laura about this. Task overtaken by events.
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.
TBD	When IR Roles doc is somewhat baked, check to see if IR Templates contains a template for each function in IR Roles.	Closed	
Alan, Hannah	Continue with IR roles and include in Handbook	Closed	
Tom + Romain + ??	Continue work on IR Handbook	Closed	
Nicole	Peruse NGI Trust funded projects to identify any that may be relevant for Sirtfi.		

Romain	Draw picture of hierarchical structure of large scale (federated) IR, including processes to join branches and leaves to the hierarchy.		
Christos	Propose a REFEDS 2020 Work plan item focused on understanding and potentially "regulating" proxy IdPs.		
Laura	Propose an ACAMP session on stakeholder expectations of Sirtfi.	In progress	
Hannah	Sirtfi 'ad' for eduGAIN website (aimed at Fed Ops). All to provide comments. https://docs.google.com/document/d/1trIFfKHC9lTlFMW0tI25r9q8KL4LLHmuhtHzV1Z_4x4/edit#	In progress	
Hannah	Ask Davide whether security contacts for Fed Ops exist	Done	Yes (WIP) https://technical.edugain.org/status
David G, Uros	Improve sharing procedures in AARC DNA3.2 paper by folding in experience from EGI.		

October 24, 2019

Attending: Tom, DavidG, Hannah, David K, Alan B, Uros, Shannon

Regrets: Scott, Pål, Romain

Agenda:

1. Task review
    a. If Romain can join us, let's discuss his model for large scale IR that figured in his presentation last week at the NSF Cybersecurity Summit.
2. New task: Incremental addition to the AARC DNA3.2 paper based on table top feedback.
3. Update on prospects for new table top exercises.
4. Status of Sirtfi+ Registry incubation project.
5. Any plans for Sirtfi at TechEx? Submit proposal for TNC20?
6. AOB

The group focused on agenda item #2, guided first of all by Hannah's list of table top feedback items recorded in her comment in the AARC DNA3.2 paper attached to the Executive Summary. Point-by-point discussion covered:

- The templates Hannah worked on for the WG may suffice, perhaps with a little tweaking. But those seem in fair shape.
- The templates include one to acknowledge receipt of information.
- We decided to start with the procedures towards the end of AARC DNA3.2 paper rather than starting from scratch, and recognized that we'll eventually want to pull operational, procedural, practical stuff from the final paper into a separate doc to be used as a practical aid to those coordinating an incident or performing some other role.
- We spoke about the kinds of trade-offs to be managed in deciding whether to share what info when with whom. These include:
    - Undersharing can reduce the amount of useful info available to the IR team by not enabling more sites to contribute info.
    - Undersharing and opacity can undermine trust in the IR team.
    - Oversharing can compromise incident management by exposing info to an adversary.
    - Oversharing can intrude on each affected organisation's management of its own reputation.

  David G and Uros agreed to start by improving the guidance to Coordinators in the AARC DNA3.2 paper on sharing of information during an incident, in particular taking into account EGI's guidance to Coordinators in section 5 of their Security Incident Response Procedure.
- We tabled discussion of selecting or switching Coordinators until Romain can describe his large scale IR model and experiences. It was recognized that each organisation, such as a site, federation, or research e-infrastructure, has (or is presumed to already have) established IR procedures, roles, and tools, and that whatever we do to coordinate between these existing "trust domains" must respect and complement that. In particular, as an incident is seen to cross into a new domain, that domain will coordinate IR activities within it following its established procedures. There might not be an uber-coordinator.
- We wondered if the eduGAIN Security team have already recognised a need to have accurate security contact info for member federation operators. Hannah will check with them. [She did, they do, work in progress.]
- The table top feedback includes an item about knowing the fed op of a given entity. Digging a bit, the reason why is that a Coordinator and a security contact at some entity may not be known to each other, no prior trust relationship has been established. Hence, the Coordinator should coordinate delivery of their info via a trusted intermediary. This was presumed to be the "right" fed op during the table top, but in fact the need goes beyond federations. To e-infrastructures certainly, and further as the federated access/FIM ecosystem evolves further. It was noted that proxies compound the problem

by making it a bit more difficult to trace back to affected entities. We agreed to return to this in the context of Romain's looked-for presentation of his large scale IR model.

- We punted, for now, the item about tool for secure communication of confidential info, beyond recognizing that each domain participating in an IR will use its own for its internal coordination.
- We added one item to the feedback list: a way for those who have not been notified by a Coordinator, but wonder if they may also be a target, to act on this question.