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

May 21, 2020

Attending: Tom, DaveK, Laura P, David C., Alan B, Shannon R

Regrets: Hannah, Pål, Mario, Sven, Uros, Romain (it's Ascension Day in several EU countries)

Agenda:

1. Question to Romain and Marina: has this WG given all the feedback you need for the IR Handbook?
2. IR Handbook implementation support. How should this WG and/or others help prepare everyone to play their IR roles?
   a. Has technical.edugain.org been updated to publish per-federation security contact info? Is there a process to maintain that info?
   b. Is any tooling needed to support AMBER or RED notifications being sent to groups of Federation participants and Federation operators?
   c. Slack/Mattermost channel used by the IR team, as a place for IR participants to ask questions and coordinate?
   d. Who will promote the IR Handbook to Federation operators to incorporate into their security procedures/policies?
   e. Will someone provide materials for Federation operators to distribute to their members to help Federation participants incorporate the IR Handbook into their security procedures/policies?
   f. Other?
3. Does the WG believe that the IR Handbook sufficiently fulfills its deliverable of "Define incident response procedures for federations, including communication templates, and support the community in their adoption"?
4. Next task for this WG
5. AOB

(a) Will wait until a Geant person attends a call.

(b) Some members discussed the difficulty they've experienced in trying to keep extremely sensitive information in only the right hands. Problems using REN-ISAC (insufficient overlap with InCommon participation), people at security contacts being unfamiliar with TLP and unaware that someone has attested to Sirft compliance on their behalf. Sometimes such info is shared in a chat system like slack, avoiding issues with keeping something private using email. OTOH, often those with whom you want to exchange TLP amber or red info already know what that means, ie, with experienced security people. Should each fed op have something established ahead of time to which IR team members can quickly be added? Periodic testing of sirtfi contacts should be used to improve awareness by security teams that they're tagged as sirtfi compliant and understand TLP. Also, that tends to make them become a recognized source of security related messages.

(c) WG will suggest to eduGAIN security team to create a slack channel for each incident and add fed ops to it as they become involved in the incident. Fed ops should be encouraged to decide ahead of time how they'll handle such communication with members of their federation who become involved in an incident. Some form of exercise, perhaps associated with periodic security contact maintenance, helps reinforce usefulness when a real incident happens.

Action Item: Tom suggest to eduGAIN security team as in (c) above. [20200521: Done]