Sirtfi WG google folder:

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

Task List

Who	What	When	Status
Nicole	Collect several fed security plans.	Done	https://wiki.refeds.org/display/GROUPS/Federation+Incident+Response+Plans Notes: FOs don't sign up for Sirtfi - do we need a template / criteria for involving them in incident response? Is the AARC doc the right set of template things we want them to do? https://aarc-project.eu/wp-content/uploads/2017/02/DNA3.2-Security-Incident-Response-Procedure-v1.0.pdf
Nicole	Check with WAYF on how they do their incident response - is it like other hub and spokes?	Feb 28	Request sent. Response pending.
Shannon	Report on REN-ISAC information sharing guidelines (2.d)	Done	REN-ISAC ISP Public, Limited, Privileged, Restricted Use information are of interest
Romain	Gather IR plans from some e-infrastructures	Feb 6	
Hannah, Romain	Update templates with experience from table tops. Hannah and others have already outlined these in another report. Place	Done	Initial set in in IR Templates subfolder

	results in subfolder of the sirtfi google folder, for now.		
Laura	2.c Incident response team communication: Outline a set of requirements for a communications tool (to help with tool selection)	Done	Held a session during the TIIME meeting where the group provided a set of tool requirements and some suggestions of tools. NOTES
Mario	Brief Geant 4-3 IR meeting attendees on Laura's task, maybe arrange Laura's remote participation		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.
Shannon, with input from Doug Pearson	Bullets that describe how REN sharing agreement doc should be transformed for (1) federated IR management team context, and (2) broader notification, sharing, or publishing		"user stories", problem description. Pending discussion with Doug.
Scott	Contact InCommon to see if keeping security contact information fresh could become part of baseline requirements, and use InCommon to investigate and draw out both the policy and the technical implementation. Keep Nicole, Laura, Mario, and Pål in loop. Mary-Catherine Martinez <mc.martinez@innosoft.ca> is Community Trust and Assurance Board chair.	Done. Initial email sent to Mary-Catherine Martinez	
Nicole	Prepare to operate sirtfi.org website - eg, make it a blank wordpress site	Done for now	Registered by Scott, discussed transferring
Nicole	FOs don't sign up for Sirtfi - create a template / criteria for involving them in incident response		
Laura + conscripts	Distill essential requirements from TIIME tool talk (Laura's item above) and identify one or two possible solutions		Sorry I can't be at the meeting on 3/14. I'll give an update at the next meeting.

TBA (Nicole?)	Promote “Transits” CSIRT training to (some) FOs. Possibly compress that 3 day event into 1.5 days or so. Who should take this earlier? eduGAIN support? Some specific FOs?		
Tom	Create user stories doc in Sirtfi WG folder, add Shannon’s, and WG members add to it as stories occur	Done	Doc created.
Tom	Clean up WG task list on the wiki	Mar 28	Done
*	Add user stories to the doc.		
Alan, Hannah	First stab at thinking through Per Role docs		Draft IR roles doc started. It’s really interesting, everyone take a look!
Tom	Draft outline of IR for R&E Feds		April 25: On vacation, no progress
Hannah	Add a User Story about wider notification of lessons learned & recommendations based on the incident experience.	Apr 11	Done
Hannah	Updates to IR templates as discussed on March 28		All but done
Uros & Christos	add more material to the User Stories		
TBD	When IR Roles doc is somewhat baked, check to see if IR Templates contains a template for each function in IR Roles.		
Nicole	Add use cases to the User Stories as appropriate to describe the types of scenarios/obstacles encountered in the recent incident discuss on the Apr 25 WG call.		

April 25, 2019

Attending: Tom B, Romain W, Alan Buxey, Scott K, David G, Laura P, S. Roddy, Nicole H, Brook S

Regrets: Uros, Hannah

Agenda:

1. Review open tasks
   Updated the status of some tasks above.

2. New tasks
   One for Nicole - see above.

3. Other business

We spent most of the hour discussing a recent incident, highlighting some of the obstacles to getting actionable information to the right parties in a timely fashion. TLP was observed in this discussion - have no worry! Sirtfi's work might not be able to fix it all, but it is very clear that what we do can significantly reduce the amount and nature of obstacles that currently inhibit information sharing and incident management. Among them:

- A tool/channel at the ready so that individuals that need to share can do so.
- Sharing guidelines and templates right there to minimize the problem of figuring out how to share what with whom over that channel.
- Sharing guidelines about how to share what with whom in a broader way, as such info is developed. Here, "broader" means among sets of people beyond those managing an incident, hence not privy to the most sensitive forms of incident information, but short of "public". Ie, those who "need to know", if we can figure out an approximate answer to that.
- Operational support to make the above happen. Tom will speak with leaders at Internet2 about discussing this with their counterparts at GEANT.

Scott also observed how the incident we discussed re-emphasized the need for us to develop Sirtfi v2, whose chief enhancement over v1 is the obligation of an entity operator to suitably notify others when they become aware of a compromise associated with their entity.