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		First attempt done

	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 people of 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
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.		
Nicole	Prepare to operate sirtfi.org website - eg, make it a blank wordpress site		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		
Tom	Clean up WG task list on the wiki		

March 14, 2019

Attending: Tom, Hannah, Scott, Shannon, Pål, Alan Buxey

Regrets: Uros

Proposed agenda:

1. Task review
    a. Scott's task: delinquent, will attempt to get to it soon
    b. Hannah’s task: brain like a sieve. Will do it soon
2. New tasks
    a. Is it too soon to start an outline of the new paper?
    b. Rather, what are the things we’ll produce:
        i. User stories first
        ii. Incident response for federations paper, ie, enhancement of AARC paper
            1. Also cover case when an org is not sirtfi
            2. The security contact in metadata is used to bootstrap getting a live person engaged with the means we’ll identify for securely exchanging sensitive info during an incident
            3. When is each type of incident responder done with their role in managing an incident
            4. Wider sharing of information after a security incident has been managed, ie, so that others learn and benefit, and who has that responsibility
        iii. Documents aimed at each of the roles defined in 2.b.ii above, eg, one for SPs, one for FOs, etc, so that they have everything they know in one place
        iv. Template IR policies for FOs
        v. Doc focused on the secure communication tool(s) that we select. Or should this be (only) an aspect of 2.b.ii above?

vi. Sirtfi v2, maybe later on

3. Other business
    a. Question: should SIRTFI offer any input on the tension between investigation/post-mortem and just getting services back up?