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, Done	A: Surfnet style model, no english documentation, playing a heavy role in managing incidents
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,	Update templates with experience from	Done	Initial set in in IR

Romain	table tops. Hannah and others have already outlined these in another report. Place results in subfolder of the sirtfi google folder, for now.		Templates subfolder
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	June 5 2019 Scott met with InC's Community Trust and Assurance Board about partnering with them to investigate doing this. Positive response from CTAB. Small WG forming to dig in.
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 (i.e. get FOs to declare what they are doing and start actively monitoring this). Also encompasses	In Progress	Raised at Steering Committee, small WG created.

	defining what FOs should be doing during incidents.		
Laura + conscripts	Distill essential requirements from TIIME tool talk (Laura's item above) and identify one or two possible solutions.	Done	Draft tool req doc | federation survey | REFEDS discussion?
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? (Also see what material is applicable)	Done	Proposed TRANSITS in 90 minutes at REFEDS at TechEx and get feedback there on usefulness.
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. Comments are welcome!	Done	Draft IR roles doc started. It's really interesting, everyone take a look!
Tom	Draft outline of IR in R&E Feds	May 9	Initial draft outline complete
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	Done	
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 discussed on the Apr 25 WG call.		Organisations removed information from the public domain.

	Update: maybe still interesting from a process perspective even if details can't be public.		
Alan, Hannah	Continue with IR roles and include in Handbook		
Tom + Romain + ??	Continue work on IR Handbook		
Uros	Start a doc on the Sirtfi + eduTeams question, and get Christos to explain it to us.	Done	Started Doc
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.		
Hannah, Christos, Alan	Brainstorm good, bad, and ugly potential resolutions to the question that Uros and Christos brought to the WG, as described in the August 1 2019 notes below and in Proxy asserting Sirtfi as an IdP.	Aug 15	

August 1, 2019

Attending: Tom, Sirtfi, Dave K, Christos K, Shannon R, Uros S, Scott K, Hannah S, Laura P, Alan B

Regrets: Romain

Agenda:

1. Review open tasks
2. Discussion
    a. Christos Kanellopoulos: Sirtfi & eduTEAMS
    b. Other
3. Follow-up actions

    a. Christos, Hannah and Alan (when he's back from holiday) to write up a brief report of the Community AAI pseudo-proxy system and way forward.
4. Other business

The WG read Proxy asserting Sirtfi as an IdP, the doc that Uros and Christos wrote to set up the discussion, then Christos described steps taken and the situation with eduTEAMS and its community AAI, which functions as an IdP/OP to SPs associated with a given eduTEAMS-supported research community. Some of those SPs can be SPs that are also registered in R&E Federation, and their use case centers around users who access that SP as a member of that research community rather than as a member of their home organisation, whose IdP performs actual authentication to the eduTEAMS AAI. In this situation, the SP receives authentication and attribute assertions/claims directly from the eduTEAMS AAI. Those claims are based on aspects of the user's membership in the research community as recorded in their eduTEAMS profile, which itself may incorporate information supplied by the user's home organisation that is relevant to the eduTEAMS AAI, either as assertions/claims about the user or via entity attributes in the home organisation IdP's federation metadata.

Imagine what happens when the SP operator notices something odd, begins to investigate, and determines that the Subject implicated in the suspicious behaviour was given its SP session and security context based on attributes/claims it received from the eduTEAMS AAI. They contact the eduTEAMS AAI security contact, and continue the investigation together. If the eduTEAMS operator determines that the investigation needs to involve the Subject's home organisation, they contact its security contact.

If all three, SP, eduTEAMS AAI, and home organisation IdP, assert Sirtfi, all is well. The question raised by Uros and Christos is what should happen if the home organisation IdP does not. From the perspective of the incident response, they will proceed to work with that IdP as best they can, of course, even if the Sirtfi specs aren't all met.

But consider the situation when the SP's policy is to only permit user access when Sirtfi compliant measures protect their IdP. The eduTEAMS AAI's IdP is tagged Sirtfi, and that's where the SP got its claims from. Does eduTEAMS meet the full intent of Sirtfi if some of the home organisation IdPs of users in its supported research communities don't assert Sirtfi? Is there some way that it can handle that situation and fully meet Sirtfi?

The Sirtfi spec did not take this situation into account, ie, the use of Sirtfi as an element of user access policy at an SP, together with multiple entities involved in the assertions/claims received by that SP. Is some modification to Sirtfi needed, or advisable, to address this use case and clarify how the eduTEAMS AAI can meet the intent of the SP's user access policy?

Hannah, Christos, and Alan agreed to brainstorm some possible remedies offline and will bring their ideas to the WG at its next meeting. Also offline, Tom asked them to avoid trying to decide on the best or right approach and instead identify as many good, bad, or ugly solutions as they

can imagine. That way the WG as a whole can best consider what resolution they would like to bring.