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		

July 4, 2019

Attending: Hannah, Uros, Nicole, Alan (****Sirtfi Independence Group****)

Regrets: Tom, Scott

Agenda

1. Review open tasks
2. TNC debrief
    a. Tom's REFEDS WG update
        i. Especially slide 6, which reflects items noted in the nascent IR Handbook
            1. Nobody seemed particularly pro or against
            2. Sirtfi WG to send someone to join eduGAIN security group meetings
            3. REFEDS is probably not a sustainable place to fulfil these requirements
            4. Believe that FOs are more or less on board, would like someone to run with it
    b. Security Day side meeting
        i. Crisis exercise for eduGAIN discussion
            1. General positive response, good engagement with the activity
            2. Would need to balance content/technicality with cost
            3. Timeline = next few years
            4. Could build on the previous simulations
            5. Should raise awareness of value of identity federation
            6. Hannah to meet with Charlie in August to summarise and hopefully present at next REFEDS to gauge interest
    c. International Baseline discussion start (Sirtfi may be an element)
        i. Picks up on eduGAIN working group, targeting TechEx to discuss more
        ii. Also discussion on baseline applicability to federations/entities, and possibility to exclude
    d. Other?
        i. Discussion that eduGAIN steering group might be made open to observers

        ii. Sirtfi stickers were good :)
        iii. Noted that the attribute release webinar was nice and would be good to run at federation level
3. Open work items - can we assign some next steps?
    a. Work on IR Handbook sections or Appendices
        i. Alan & Hannah continue work on IR roles document
    b. Draft information sharing guidelines (@Tom, not really sure about this bit. we think this is at a fairly deep level, along the lines of REN-ISAC, but not quite sure)
        i. Among IR Team members
        ii. Broader dissemination of non-confidential information
4. Tools discussion - resolution?
    a. An IR Team is iteratively assembled in response to a federated incident. They need tools to help them work together, necessarily distinct from any tools any organisation already uses.
        i. Secure chat
        ii. Secure file drop
        iii. Others?
            1. Identity verification (in an easy way, considering email signing is not ideal, and that an IdP might be down as part of an incident)
            2. Suggestion from Nicole to ask NGI Trust to come and give us a presentation (very early startup)
    b. The possibility of tools for proactive notification is queued until the WG's Phase 3 of work (we're in Phase 2).
5. Other business
    a. Should discuss how proxies can assert Sirtfi compliance for certain identities coming from Sirtfi compliant places

Actions:

- Hannah ask Tom if willing to have presentation from NGI Trust on digital identity proofing