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.		
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.		

July 18, 2019

Attending: Tom, DaveK, Uros, Romain, DavidG, Shannon, Nicole, Laura Paglione

Regrets: Alan Buxey, Hannah Short, Scott Koranda

Agenda

1. Thanks to the Sirtfi Independence Group for carrying the torch last meeting!
2. SLATE - an interesting use case, new security-oriented WLCG WG spinning up
    a. Proxied by CILogon
    b. Itself an infrastructure being deployed across sites. Goes beyond WLCG, EGI, OSG, campus science DMZs, ...
    c. *If there's an incident involving SLATE and federation, how should appropriate people be identified and added to the corresponding (Sirtfi) IR Team? What if there are other IR teams responding to the same incident?*
    d. IR Handbook, IR Roles, might be useful, as will a formal trust framework for SLATE, or perhaps other things much like it. WLCG WG to consider such matters.
3. Review notes, questions from last meeting

   a. Info sharing guidelines
   b. How proxies can assert Sirtfi compliance for certain identities coming from Sirtfi compliant places
   c. NGI Trust
4. Review open tasks
5. Other business

Much of the time was spent discussing the SLATE situation as a more complicated circumstance across which an incident response may need to be mounted. The discussion helped illuminate interests held by different stakeholders in the health of the federation and how federated IR procedures might or might not accommodate them. In particular, we decided to pick this back up again when the WG focuses on the information sharing guidelines and on the process for raising awareness of suspicious behaviour, ie, that may result in additional people joining an established IR Team. Further, Romain agreed to draw some pictures that may help us better understand some of the dynamics of the IR process/workflow and structure and hence help us see how those do or can be adapted to address stakeholder interests.

The review of questions raised at last meeting led to two of the three tasks assigned (in the table above) during this WG call.

Romain and Tom will sidebar to take next steps with the IR Handbook after Romain returns from holiday.