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		Draft tool requirements document

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 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		All but 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 discuss on the Apr 25 WG call.		

May 23, 2019

Attending:

Regrets:

Agenda:

1. Review of Incident Response Communication Tools requirements
2. Other business

May 9, 2019

Attending: Alan Buxey, Tom, David G, Hannah, Uros, Pål, Scott,

Regrets: Romain

Agenda:

3. Review of tasks != draft outline of IR in R&E Feds
4. Review draft outline of IR in R&E Feds.
    a. Good resource: SANS Incident Handlers Handbook
        i. Refer to SANS incident handling - notes for a check on how our proposed preparations stack up against the SANS recommendation.
    b. What should be added?
    c. What should be removed?
    d. What should be altered? Make comments/edits in the doc.
    e. Next steps
5. Other business

Laura to lead the group in a discussion of priority of tool requirements at next meeting. That should position a set of people to assess a set of prospective tools and bring their conclusions back to the WG, and likely to share widely, but also specifically with Internet2 and Geant T&I leadership.

General agreement on the handbook approach to the IR in R&E Feds doc. Observed that as it will be long, important to break out those pieces that someone needs to know when they need to know it, as part of the objective of minimizing the time to respond to an incident. A number of suggestions and thoughts were incorporated into the draft doc.

Several new use cases were added to which the doc should be responsive.

Suggest to Internet2 & Geant T&I leadership that they add some APAN partner to their discussion of Fed IR support.