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	Review Mar 28	First attempt done, 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 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. 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.		
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		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		Doc created.
Tom	Clean up WG task list on the wiki		
*	Add user stories to the doc.		
Alan, Hannah	First stab at thinking through Per Role docs		
Tom	Draft outline of IR for R&E Feds		

March 28, 2019

Attending: Alan Buxey, Hannah, Tom, Uros, Christos, Shannon

Regrets: Pål, Romain

Agenda:

1. Feedback from Romain’s SIRTFI talk at HOW19 last week.

   Observed that InCommon’s high adoption of security contacts is one element of its Baseline Expectations program.

   Referring to one of Romain’s observations about the presentation, some WG members speculated about the nature of concern expressed by a DOE labs person about sharing incident info. Might be worthwhile to ask about it, especially to take into account in developing information sharing guidelines as part of Sirtfi.

   Discussion about the nature of Snctfi and its relation to Sirtfi. Left unresolved for the moment to return to the agenda, but we may need to revisit as it seems apropos to our purpose in defining how IR should proceed across Feds, and research proxies are in that picture.

2. Task review

IR Templates

- remove email pgp signature and headers, keep just the message body
- Mark areas to be filled in with yellow highlighter and include instruction at top to replace the marked areas with actual text, replacing any illustrative text within
- [Hannah] Add a User Story about wider notification of lessons learned, recommendations based on the incident experience.

3. Confirm whether the following is the complete set of documents we'll produce as part of the current arc of work:
    a. *User Stories*
    A compilation to be used as a check on completeness of the materials produced by the WG. Working Group members should add stories to this compilation as they occur to them.
    b. *Incident Response in R&E Federations*
    A paper to replace or enhance the AARC DNA3.2 paper. It will define roles and responsibilities of various parties in managing federated security incidents, information sharing guidelines, tools, procedures, and templates.
    c. *Per-Role documents*
    Highly desired to produce documents, one per role defined in Incident Response in R&E Federations, that lays out everything someone in that role needs to know, in one place.
    d. *Template IR Policies/Procedures for Federation Operators*
    Provide one or more starting points from which FOs can build up their own IR plans.

    Some question about template IR policies/procedures for FOs - would they be determinant from IR for R&E Feds. We opine that there will be overlap but perhaps FOs may have a wider range of circumstances to address in their own IR procedures.

    e. Sirtfi website
    A place to publish the above docs, publish information to be shared TLP White. One-stop shop for R&E Fed IR.

All agreed on the above as a reasonable spanning set of docs.

4. Editors for each of the above, i.e., who will take the next steps.
    a. Nicole has (d)
    b. Alan and Hannah to take a swipe at sketching the Per Roles docs
    c. Tom will outline the IR for R&E Feds doc
    d. Uros and Christos to see about adding more material to the User Stories, not leaving that solely to WG members when something occurs to them

5. Should/can we provide translations for each of the above into several languages? If so, which languages?

   Only 1 minute left for this item, mainly just long enough to register perplexity!