

Sirtfi WG google folder:

[https://drive.google.com/drive/folders/13EhgPxzLy4U6FMP\\_cVDalbqju40hOhUR](https://drive.google.com/drive/folders/13EhgPxzLy4U6FMP_cVDalbqju40hOhUR)

## Task List

Who	What	When	Status
Nicole	Collect several fed security plans.	Done	<a href="https://wiki.refeds.org/display/GROUPS/Federation+Incident+Response+Plans">https://wiki.refeds.org/display/GROUPS/Federation+Incident+Response+Plans</a>  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? <a href="https://aarc-project.eu/wp-content/uploads/2017/02/DNA3.2-Security-Incident-Response-Procedure-v1.0.pdf">https://aarc-project.eu/wp-content/uploads/2017/02/DNA3.2-Security-Incident-Response-Procedure-v1.0.pdf</a>
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	<a href="#">REN-ISAC ISP</a> 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 <a href="#">IR Templates</a> 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. <a href="#">NOTES</a>
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		<a href="#">"user stories"</a> , <a href="#">problem description</a> .  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 < <a href="mailto:mc.martinez@innosoft.ca">mc.martinez@innosoft.ca</a> > 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		
Laura + conscripts	Distill essential requirements from TIIME tool talk (Laura's item above) and identify one or two possible solutions.		<a href="#">Draft tool req doc</a>   <a href="#">federation survey</a>   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?		
Tom	Create user stories doc in Sirtfi WG folder, add Shannon's, and WG members add to it as stories occur	Done	<a href="#">Doc created.</a>
Tom	Clean up WG task list on the wiki	Mar 28	Done
*	Add <a href="#">user stories to the doc.</a>		
Alan, Hannah	First stab at thinking through Per Role docs		Draft <a href="#">IR roles doc</a> started. It's really interesting, everyone take a look!
Tom	Draft outline of <a href="#">IR in R&amp;E Feds</a>	May 9	Initial <a href="#">draft outline</a> complete
Hannah	Add a User Story about wider notification of lessons learned & recommendations based on the incident experience.	Apr 11	Done
Hannah	Updates to <a href="#">IR templates</a> 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: Laura (chairing), Scott, Alan Buxey, Uros, Romain, Shannon, David G, Mario,

Regrets: Tom, Hannah

Agenda:

- Review of [Incident Response Communication Tools requirements](#)
- GEANT43 - evaluating tools - will share the information later with everyone
- Other business

Notes:

Previous tabletop exercises showed the need for some type of communication tool and drove a conversation during TIIME, which has then led to this effort to find a way to evaluate tools.

Expect resistance from people because they often want to use tools they have already used.

Most notes taken in the [Incident Response Communication Tools requirements](#) document.

- Key takeaways
  - Selection of a tool may be premature - the problem we are trying to solve may need further clarification before a selected tool would be adopted
  - Cultural & regional choices and norms are critically important. These factors will influence behavior in the moment of an incident, even if a different tool had been agreed upon. Is it important to try to change this, or do we take this as a given and determine how to work within this reality?
  - There are other tools that might have greater adoption right now, for example, automated tools that can share information about compromised accounts.
- Next steps
  - Develop a survey (distributed through the REFEDS mailing list) to understand what tools federations (and other) are using for incident response communication. As part of the survey also gather other info like why they selected this tool, how they use it, and how well it works for this purpose.
  - Get an agenda item on the REFEDS meeting at TNC to talk about the tool evaluation document and get feedback, particularly from federation operators.