Task List

Who	What	When	Status
Nicole	Collect several fed security plans.	Feb 28	
Nicole	Check with WAYF on how they do their incident response - is it like other hub and spokes?	Feb 28	
Shannon	Report on REN-ISAC information sharing guidelines	Jan 31	

January 17, 2019

Attending: Tom, Hannah, Romain, Nicole, Shannon, DavidG, Uros, Brook, Pål

Proposed Agenda:

1. Any new WG members joining us for this task?
2. Orientation to AARC DNA3.2 paper.
    a. It's our copy - ok to make comments!
    b. Go to the Table of Contents. Note 3 main parts of the paper:
        i. Background and education
        ii. Proposal for incident response
        iii. Appendices with suggested procedure and message templates
3. What needs to be added? Some possibilities:
        i. Improvements to procedures and templates
            1. Hannah's comments in the paper
            2. steps to notify broader security community. Eg, REN-ISAC.
        ii. Expansion of the proposal to cover more types of parties to an incident response
            1. Many entity's security contacts are some CERT, not the org itself.
                a. GARR, Surf, maybe other or all hub and spoke feds
                b. Some individual contacts, not generic
                c. May need to develop R&E focused subgroups of existing CERT orgs, eg, FIRST
                    i. Geant 4 project - Nicole will keep us updated
                d. REN-ISAC? Not well aligned with federation, nor substantial overlap with InCommon membership. OTOH, may be useful in more ad hoc manner, especially for broader notification of incident details.
        iii. Establishing technical means for sharing incident info among responders
            1. Eg: shared Box folder + async real-time

        a. SWITCH uses Mattermost (slack-like) https://mattermost.com/
        b. Discord https://discordapp.com
    iv. Sharing guidelines: what can/must be/not be shared with whom when?
    v. Annual table tops
        1. Romain is involved appropriate Geant project and will liaise for us
4. Is what we'll produce an enhancement to this doc or a new doc that responds to it?
5. What date should we work toward for completing this work?
    a. AARC wraps up end of April, gets harder for some to participate
6. Whose input do we need to complete the work?
7. Whose buy-in do we need to make it implementable?
    a. eduGAIN
    b. AARC DNA 3.2 authors (incl. SCI people)
8. Next steps.
9. Any other business.

REFEDS survey: lots of feds have security plans. Asked for where they are.
Should WG provide a template? -- Yes