

Consultation: eduGAIN Security Incident Response Handbook

 This Consultation opens on 20th July 2020 at 13:00 CEST and will close on 11th September 2020 at 17:00 CEST.

Background

The REFEDS Sirtfi Working Group, in conjunction with the eduGAIN Security Team, have prepared a Security Incident Response Handbook for the eduGAIN service. The document defines the roles and responsibilities of each party taking part in the Security Incident Response process that is when a Federation Participant suspects a security incident affects its resources and has reason to believe that Federation Participants outside its origin federation may be affected. The groups are now seeking feedback on this document.


Please note that while the REFEDS Consultation process is being used, the full formal consultation process for REFEDS will not be applied as this document is specific to the eduGAIN service. Comments will be processed and considered by the Sirtfi Working Group but ultimately acceptance of the document will lie with eduGAIN and not the REFEDS Steering Committee. This consultation will be shared on both the REFEDS and eduGAIN lists.

Overview

This consultation is open from: **Monday 20th July 2020 at 13:00 CEST to Friday 11th September at 17:00 CEST**

Participants are invited:

- to consider the proposed eduGAIN Security Incident Response Handbook.
- to propose appropriate changes / challenges to the propose text.

 The document for the consultation is available as a [Google doc](#) or as a [pdf attachment](#). All comments should be made on: consultations@lists.refeds.org, added to the google doc as a suggestion or added to the change log below. Comments posted to other lists will not be included in the consultation review.

Change Log

	Line Number / Reference	Proposed Change or Query	Proposer / Affiliation	Action / Decision (please leave blank)
1	152, 180, 205	"labelled TLP AMBER or higher"; not sure how to interpret 'higher' in the context of colours, assume higher means that GREEN and WHITE are also ok but RED would not. Might be good to use more explicit wording.	Thijs Kinkhorst, SURFconext / SURFcert	
2	159	Unsure why "inside one federation" must be reported to the eduGAIN security team. If there's an issue with one idp and one sp both inside the federation and no relation to any eduGAIN service, I see no need to involve more parties than necessary to solve the issue. Involving more parties has costs and should not be done if there's no clear role for the party in the ongoing incident. Propose to delete: " <i>whether inside one federation or</i> ". There's always paragraph 182-184 that states that you <i>can</i> involve the eduGAIN security team at any time when you need its help.	Thijs Kinkhorst, SURFconext / SURFcert +1 Nicole Harris, GÉANT +1 Pål Axelsson, Sunet	
3	General	What is the authority of the handbook? Is it best practice recommendations or will the statements be REQUIRED for federation participants? Needs to be stated more explicitly in the document	Nicole Harris, GÉANT +1 Alex Stuart, UKfederation	
4	Scope	What is the scope of incidents that you expect to be reported to eduGAIN? Any security incident involving the organisation or service in question or those that directly have an impact on federated identity? This isn't clear in the document.	Nicole Harris, GÉANT	

5	159	Agree with Thijs Kinkhorst proposed change, to delete " <i>whether inside one federation or</i> ". We would likely prefer not to involve a Federation Operator for incidents within our federation and just coordinate directly with the other party.	Robert Heren, University of Illinois	
6	Supporting documents	The eduGAIN Security Handbook is a very good tool but it needs supporting documents like simple checklists for the different parties.	Pål Axelsson, Sunet, on behalf of Sunet CERT	
7	150-152, 178-180, 204-206	Echoing Thijs in comment #1, I think the wording could be made clearer regarding the reports that are to be distributed under the TLP. I can understand why a TLP:Amber report should go to all affected organisations, and a TLP:White report could inform the whole community. However, the dissemination of information to "Sirtfi-compliant organisations in all affected federations" does not make sense to me.	Alex Stuart, UKfederation	
8	150-152, 178-180, 204-206	Like Thijs and Alex, I'm concerned about the references to the TLP protocol. "Higher" than TLP:AMBER in my book would be TLP:RED, which means highly confidential for a small group of people, mostly delivered orally, "for your ears only","should not leave the room". TLP:AMBER is for involved federations, a report for the whole community should be TLP:GREEN whilst TLP:WHITE is for public/press.	Henrik Larsen, WAYF, DeiC	