

Dear Sally and Dear DW

I am currently working on a new open source programme called FOSSEPS, this time externally focussed towards European Public Services, or public administrations. Here we are (i) building an open source EU Business Applications catalogue, pulling together data from a number of national catalogues. This way people can reuse, rather than re-build the same application all over again! (ii) We are also asking European Public Services and selected others (this includes yourselves, the ASF) to help us identify software projects that are in a state of critical health... i.e. in ICU, and may not survive. So, they are also critical, in that we rely on their continued existence, to run our other systems. (iii) we want to encourage European public administrations to work together on open source matters, i.e. on GovFoss.

Today, I am writing to you re #2 – Identifying Critical Software Projects. This is particularly relevant to you, given your recent experience of having to deal with the Log4shell incident. We read your position paper with great interest. We have sent out a survey and a help Guide to public administrations, but for open source experts we are holding 45 minute calls. We would be very interested in discussing your views on critical software, long-term FOSS maintenance/sustainability, and looking at security and other issues.

Sally/Dirk, would you be kind enough to identify the right people and/or send us the right information? We are looking to (i) hold a session with ASF, and so request a date/time after 28th of March, and (ii) request your list of critical software that you would have identified? In due course, we are also looking at remedies to remove such criticality and see how we can nurse these projects back to health.

----- Sample questions for the session -----

- Are there specific processes to identify projects with maintenance or security problems among Apache Software Foundation projects?
- Do you have a specific policy regarding the sustainability of the \*dependencies\* of projects hosted by the Apache Foundation?
- According to your experience, what are currently the main challenges or problems related to FOSS maintenance/sustainability?
- What are the most promising initiatives for finding solutions to those problems or taking up those challenges today? (both from a security point of view and from a maintainers' financial/mental health sustainability point of view?)
- Do you feel that there is a need for more commonly agreed metrics or publicly available sources of data to assess the health of open Source projects?
- As seen from the outside, it seems to us that the Executive Order on Improving the Nation's Cybersecurity had a key role in the progress currently being made: in your opinion was the political decision actually decisive or was it just one amongst many converging factors?
- More generally, would you consider that governments/public bodies should take specific actions on this topic?

----- end -----

Regards

Saranjit ARORA

Senior Consultant/Project Manager (Working Mon-Thu) Member of the European Commission OSPO (Open Source Programme Office) Project Manager of FOSSEPS (Free and Open Source Software for European Public Services) Pilot Project Previously Project Manager of the EU-FOSSA 2 Project and the project dealing with Open Source Software Inventory, Security, Sustainability and Funding Initiatives for European Public Services within the 2020 ISA2 Sharing and Re-use action (2016.31)

European Commission

DG Informatics, Unit B.3 – Reusable Solutions, MO15 06/P010, B-1049 Brussels/Belgium (phone # / signal / telegram redacted)