GETTING THE KINKS OUT OF THE SOFTWARE SUPPLY CHAIN

with

SPDX™
SOFTWARE PACKAGE DATA EXCHANGE®
Panelists

- Phil Odence, Black Duck Software
- Steve Cropper, Cisco
- Mark Gisi, Wind River
- Scott Lamons, HP
- Jack Manbeck, TI
WARNING: Time to Collaborate

- Who has heard of SPDX?

- Who is involved at least at the level of being on one of our mailing lists?
Software Package Data Exchange® (SPDX™)

- A standard format for communicating the components, licenses and copyrights associated with a software package.
- Key pillar in Linux Foundation’s Open Compliance Program which comprises:
  - Tools, Self-Assessment, SPDX, Rapid Alert System, Training, Community
The Need

- Our suppliers aren't giving us complete licensing information for open source packages.
- I don't mind vetting our code, but I'm sure this imported package has been analyzed a dozen times before.
- Every customer wants a bill of materials in a different form.

We need a standardized, adopted format for a software Bill of Materials.
Solution

- A file format for license information to accompany open source packages

- Benefits
  - Allows easy exchange of license information between companies
  - Avoids due diligence redundancy
  - Ultimately yields better compliance with less effort
SPDX™ Group

- A working group of Linux Foundation
- History
  - A grass roots effort started by corporate counsel, business leads, and release managers responsible for ensuring release compliance with applicable licenses of FOSS included in the release
- Operation
  - Like an open source project
  - Three teams
  - Spdx.org
Status

- Version 1.0 – Released August 2011
- Version 1.1 – Q2 2012
- Version 2.0 – Targeted H2 2012

http://www.spdx.org
DISCUSSION

Please join in