



DATA SECURITY SPECIALIST CONSULTING-CONTRACTOR OPPORTUNITY

The Open Voice Network, an open-source community of the Linux Foundation, is dedicated to the development of technology standards and guidelines that will make the emerging world of voice assistance worthy of user trust. The Technical Committee of the Open Voice Network has chartered a Technical Committee Working Group to explore and recommend guidelines on issues of **user privacy and organizational security** that may be unique to or revealed through the use of voice assistance.

The **Data Security Specialist** will advise, guide, and serve as a primary author/editor for the development and delivery of the Open Voice Network (OVON) **Security Capabilities Report v2.0** document. To do so, the Data Security Specialist will work both independently and collaboratively with teammates from around the world in regularly scheduled conference calls.

The Data Security Specialist will execute the below deliverables to the Open Voice Network as a consulting independent contractor and receive compensation through a Contractor Services Agreement with the Linux Foundation.

The Data Security Specialist may execute deliverables in any location where there is an internet connection sufficient for reliable video conferencing. Team meetings are generally scheduled between the hours of 15:00 and 19:00 CET. Conferencing and collaboration tools will be provided to enable connection with Open Voice Network teammates worldwide. No travel will be expected.

The Linux Foundation is an equal opportunity employer.



DELIVERABLES

Consultative and Support services will include advising and authoring the Security Capabilities Report v2.0 document. Specifically:

- ▲ Evolution of the v1.0 to a version 2.0 with an emphasis upon specific "what" and "how" guidance to enterprise practitioners and users of voice assistance in an interoperable world.
- ▲ Evaluation of the voice assistance ecosystem (on-device, cloud, web, IOT, etc.), advising the Open Voice Network Privacy & Security Work Group on 1) existing laws/standards/guidelines that exist and are applicable, and 2) gaps that must to be addressed through the establishment of industry- wide security guidelines.

EVALUATIVE MILESTONES

- ▲ Iteration 1: Review structure and content of document, and identification of areas for revision. Gather, document feedback on goals, recommendations in regards to content that may be missing or not aligned with current industry best practices. Target date: October 31, 2021.
- ▲ Iteration 2: Refinement of document. Further clarification of structure, sections, and references. Target date: November 30, 2021.
- ▲ Iteration 3: Delivery of Security Capabilities Report v2.0. Target date: December 31, 2021.

REQUIREMENTS

- ▲ 4+ years of prior relevant experience.
- ▲ Advanced certification in Information Security, Risk, or Audit certifications preferred. Examples of preferred: CISSP, CISA, CISM, CASP, etc.
- ▲ Demonstrated working knowledge of industry best practices, e.g., NIST, OWASP, ISO/IEC 27002 Advanced understanding of TCP/IP, common networking ports and protocols, traffic flow, system administration, OSI model, defense-in-depth and common security elements.



- ▲▲ Experience in analysis of complex security issues and the development and engineering activities to help mitigate risk.
- ▲▲ English-language communication (speak, write) skills, and the ability to work collaboratively with a remote global team.

COMPENSATION

This opportunity is structured to be a part-time consulting engagement with the Linux Foundation, as provided by an independent contractor. We anticipate this to be a 10-12-week engagement. Compensation will be structured in accord with expertise.

