CYBEROREGON

Oregon Cybersecurity Advisory Council (OCAC)

Historical Perspective and the Improvements in LC 295

Charlie Kawasaki, CISSP
February 4, 2022

Testimony By

Charlie Kawasaki, CISSP
Vice-Chair, Oregon Cybersecurity Advisory Council

Other Volunteer Engagements
Board Member, Technology Association of Oregon
Executive Council, OSU EECS Industry Advisory Board
Industry Advisory Board, Chair, ORTSOC
Industry Advisory Board, Cybersecurity, Mt. Hood Community College
Founder, NW Cyber Camp

Industry Engagements
Consultant, PacStar (Curtiss-Wright)
Advisory Board, 3GO Security, Inc.
Consultant and Investor, DeepSurface Security, Inc.
Associate and EIR, Bulls Run Group, Inc.
Venture Partner, Oregon Venture Fund

OCAC - History

- SB 90 was signed on 9/19/2017
- Per SB 90 OCAC submitted a CCoE establishment plan in December 2018
  - The Council has not been operational since shortly thereafter – no official business conducted
- Last of several OCAC meetings took place Oct 2020
- Council member terms are expired / expiring now
- Small workforce development/educational, awareness, and information sharing programs have continued without coordination and with limited financial support

OCAC under SB 90 vs. LC 295

- SB 90
  - Scope: Provide a State-wide forum, information sharing, advisor to State CIO, and encourage workforce development. Delegated responsibility to create CCoE plan
  - Council Makeup: 9 Members, primarily from industry. One EDU and one law enforcement person required
  - Budget: Only travel and direct expenses, to be funded from the State CIO budget. No budget was allocated for this.

- LC 295
  - Scope: Create CCoE Charter, create plan for CCoE and report on status, create planning committee for Fed grant requirements. Adopt rules for the CCoE
  - Council Makeup: 15 members with large % from underserved public bodies (Tribes, Cities, Counties, Spec. Districts, ESDs/K-12, etc.) Includes higher education, Oregon EIS department, cyber industries, and tech associations.
  - Budget: Only travel and direct expenses, to be funded by CCoE budget

Key Changes to CCoE in LC 295

- LC 295 establishes Focus #1 – Underserved public bodies
  - Assist underserved public-sector organizations and critical infrastructure. Conduct centralized assessment, planning, and recommendations. Assist in standing up solutions.
    - ***Lowered/reduced priority on addressing problems of the State Government***
- LC 295 establishes Focus #2 – Cybersecurity workforce crisis
  - Provide or fund programs that address the workforce/awareness gap – required to support Focus #1
- LC 295 Methodology
  - Convene stakeholders and experts
  - Develop detailed ***fundable and executable plans*** based on expert, and detailed bottoms up vulnerability assessments and risk management analysis.
  - Communicate the needs and plan to all stakeholders
  - Secure funding at the State and Federal level to execute those plans

The CCoE funding in LC 295 provides just enough resources to start the planning and assessment process – delivering well documented assessments of gaps and needs in public bodies. In 2022 we are asking to fund the planning process, with a very modest request.

OCAC Challenges Since 2017

- SB 90’s scope was too broad and anticipated actions and funding to support OCAC and CCoE that did not occur.
- No funds or staff were made available to support the CCoE or to support/grow existing cyber work force development programs.
- No incentives were provided for substantial private sector involvement.
- The private sector made it clear they are willing to, at most, provide occasional expert advice, discount software / online training, an extremely modest financial support. They will not provide the financial support at the scale necessary to fix the problems in the state. This requires staff; state, local and federal funding, and investments in cyber workforce development, education, training and goods and services.
- The State of Oregon CIOs office is focused on the cybersecurity needs of state government (executive branch); has not been able to provide sustained direction or staff/financial support to OCAC.

But For LC 295

- Oregon will have no coordinated approach to protecting public bodies from cyber attacks such as ransomware, and each will be left on their own to solve the problem – without the funds or expertise to do so.
- Oregon will have no coordinated workforce development plan in cybersecurity, and public bodies will continue to compete with the private sector for expensive and extremely difficult-to-hire cybersecurity staff, and/or pay extraordinary rates to sought-after consultants.

How LC 295 Fixes This

- Creates a council with interests that align with key stakeholders (public bodies)
  - Public body council stakeholders will drive OCAC and CCoE to solve their cybersecurity crisis – providing urgency and direction
- Provides funds necessary for OCAC/CCoE to ***get started.***
  - Assessing the needs of 1,500+ underserved public bodies and developing a fundable plan, at scale, will require a substantial effort.
  - Pursuing those funds at the Federal level will require a credible, functional team and organizational structure
- Provides small amounts of funding to assist with public bodies immediate needs and makes it possible to secure federal funds from IIJA.
- Provides small amounts of funding to make progress on workforce development, and to develop a comprehensive plan.

Thank You!

Charlie Kawasaki, CISSP
ck@softwarediligence.com