CHARTER

Washington State Cybersecurity Advisory Committee

I. Name

The committee's name shall be "Cybersecurity Advisory Committee," hereafter referred to as the Committee. This Committee is a subcommittee of the Washington State Emergency Management Council (EMC).

II. Authority

The Committee is authorized and empowered by the laws in Chapter 38.52.040 of the Revised Code of Washington (RCW). The Committee's annual reporting requirement is authorized in Chapter 43.105.291.

III. Purpose

The Charter identifies the Committee's responsibility to provide advice and recommendations that strengthen cybersecurity in industry and public sectors across all critical infrastructure sectors. Advice and recommendations produced by the Committee will be provided to the Emergency Management Council (EMC) and included in an annual report to the legislature.

IV. Priorities

A. Identify which local, tribal, and industry infrastructure sectors are at the greatest risk of cyberattacks and need the most enhanced cybersecurity measures.

B. Uses federal guidance to analyze categories of critical infrastructure in the state that could reasonably result in catastrophic consequences if unauthorized access to the infrastructure's information technology and/or computer networks occurs.

C. Recommend cyber incident response exercises related to risk and risk mitigation in the water, transportation, communications, health care, election, agriculture, energy, and higher education sectors. Additional sectors may be considered as deemed appropriate by the Committee.

D. Examine inconsistencies between state and federal law regarding cybersecurity.

V. Membership

A. Committee membership should include, but is not limited to, at least one representative with cybersecurity expertise from an organization in each of the following sectors:

i. Commercial Facilities
ii. Communications
iii. Critical Manufacturing
iv. Elections Subsector, Government Facilities

v. Emergency Services
vi. Energy
vii. Federal Homeland Security Agencies
viii. Financial Services
ix. Food & Agriculture
x. Healthcare & Public Health
xi. Higher Education
xii. Information Technology
xiii. Local Government
xiv. Transportation
xv. Tribal Government
xvi. Water/wastewater

B. The Technology Services Board (TSB) Security Subcommittee chair shall be a standing committee member.

C. Committee membership is managed by the Washington State Military Department's Emergency Management Division (EMD) according to the requirements of this charter.

VI. Member Expectations

A. Members should have expertise and responsibilities for cybersecurity for their organizations and/or are the lead state agency for coordination with their sector regarding cybersecurity planning, training, exercise, and incident coordination.

B. Committee members will make every effort to attend meetings.

C. If a member misses two (2) consecutive meetings without good cause, the Committee may recommend to the Emergency Management Council that a new member vacate and fill the position.

VII. Meeting Administration

A. Meetings will be scheduled, facilitated and documented by the Washington State Military Department's Emergency Management Division.

B. Meetings will be held at least quarterly and may occur at greater frequency as determined by the Committee members or the Emergency Management Council (EMC).

C. The Committee will hold at least one (1) meeting annually with the Technology Services Board (TSB) Security Subcommittee, administered by Washington Technology Solutions (WaTech).

D. Meetings will provide in-person and virtual options for attendance.

E. Meeting agendas will be created and distributed to members no-later-than two (2) weeks prior to the meeting date.

F. Meeting minutes will be distributed no-later-than one (1) week after the meeting date.

VIII. Deliverables

A. The Committee will provide a written report to the Emergency Management Council (EMC) three weeks in advance of scheduled EMC meetings.

B. The Committee will provide an annual update as part of the Emergency Management Council's (EMC) annual report.

C. The Committee will provide an annual written report to the Washington Technology Solutions agency for inclusion in a report to the legislature each December.

IX. Information Security

A. The reports and information, or any portions thereof, that are designated confidential by the Committee are exempted from disclosure under the Washington Public Records Act (Chapter 42.56 of the Revised Code of Washington).

B. Sensitive security information discussed in the Committee may use the federal Protected Critical Infrastructure Information (PCII) program to mark, protect, and maintain information security appropriately. The PCII program is administered by the Department of Homeland Security and coordinated in Washington State by the Military Department's Emergency Management Division.

   a. All Committee members must complete PCII training which is required to handle or view any material designated as PCII by the federal government. The training must be completed prior to the Committee meeting immediately following their appointment.

   b. Per PCII handling requirements, any individuals who have access to PCII information must also complete PCII training. This includes:

      i. All IT support staff, or any other staff, who administer or have access to network locations where PCII is stored.

      ii. Members of the Emergency Management Council who wish to review PCII protected documents produced by this Committee.

      iii. Coworkers, supervisors, or leadership from any organization that is represented on this Committee.

X. Amendments

This Charter may be amended, repealed, altered, on whole or part, or a new Charter adopted at the recommendation of the Committee and with approval of the Emergency Management Council (EMC).

XI. Adoption Date and Annual Review

A. Adoption Date: 1/25/23

B. An annual review is due each December.