CISO Council Charter

This CISO Council Charter (the "Charter") sets forth the purpose, membership requirements, and conduct of the CISO Council (the "Council") for the Commonwealth of Massachusetts.

1) Purpose

The purpose of the Council is to provide a forum for effective collaboration, thought leadership, insights and sharing about information security leadership, management, and practices across Commonwealth government.

2) Scope

The scope of the Council's efforts is to advise, recommend, and support Commonwealth government participants regarding best practices to identify, manage and mitigate information security risks within the Commonwealth.

3) Governance Principles

Principle 1: The CISO Council takes a blame-free, 'fix the problem' approach of community and collaboration that embraces and promotes continuous improvement guided by the Commonwealth's Enterprise Information Security Policies and Standards.

Principle 2: The CISO Council is committed to becoming advocates and ambassadors of fostering a risk-aware culture within constituent agencies across the Commonwealth.

Principal 3: The CISO Council endeavors to deliver executive level, strategic viewpoints on changes and advances in information security practices and programs in ways that benefit the Commonwealth and its many constituents and residents.

4) Key Goals

Goal 1: Risk Reduction through Risk Assessments, Awareness Training, and Remediation:
The Council will focus on improvement, introduction or development of consistent tactics, techniques and procedures across the Commonwealth.

Goal 2: Continuous Improvement of Commonwealth Capabilities:
The Council seeks to enhance the ability to preemptively discover and mitigate information security risks as well as respond effectively to information security incidents by conducting and/or engaging in periodic Cybersecurity Tabletop Exercises that simulate 'real world' security events. This goal focuses on targeting, identifying, learning and training business units throughout the Commonwealth by identifying 'sweet spots' to focus training and awareness based on current information security threat trends.

Goal 3: Maintain Information Security Vigilance:
The Council supports maintaining vigilance through both business and technical Vulnerability and Third-Party Risk Assessment and Remediation. This goal focuses on examining and improving specific areas of vulnerability ranging from

intrusion attempts and methods, vendor security ratings, patch policies (internal and third-party), and performance indicators like mean times to response and resolution.

5) Membership

Membership Qualifiers: The Council seeks key people within Secretariats, agencies, commissions, or other Constitutional offices who are charged with information security responsibilities and provide strategic direction to the staff in implementation, management and maintenance of information security within the Commonwealth.

6) Organization

a) Key Roles

- Council Leader
    - Schedules and leads CISO Council meetings
    - Sets CISO Council meeting agendas
- Subcommittee Leaders
    - Schedules and leads subcommittee meetings
    - Sets subcommittee meeting agendas
- Council Recorder
    - Takes and distributes minutes
    - Distributes CISO Council and Subcommittee reports as necessary

b) Subcommittees

The Council shall have the authority to delegate authority and responsibilities to subcommittees, so long as no subcommittee consists of fewer than two members. Subcommittees may be formed and dissolved at the discretion of the Council. Until such time as they are dissolved or amended, the following subcommittees will be formed as standing subcommittees:

- Cybersecurity Vulnerability Management
- Information Security Training and Awareness
- Information Security Strategy

c) Coordination with Home Agency

Members of the Council understand that it is their responsibility to have the readiness and capacity to advise, inform, implement and/or promote information security awareness, practices, and capabilities within their home organizations. Members are charged with representing the interests of the Commonwealth as a whole as part of enterprise information security leadership within their home organizations.

7) Meetings

a) Frequency of Meetings

The Council shall meet at least monthly - or more frequently - as it shall determine is necessary to carry out its purpose and objectives. The Council may establish a schedule for regular meetings of the Committee. The Council Leader shall schedule meetings, set the agenda, and may call a special meeting at any time as he or she deems advisable or as events dictate.

Subcommittees shall meet as necessary to carry out its purpose and objectives. The Subcommittee Leader shall schedule meetings, set the agenda, and may call a special meeting at any time as he or she deems advisable or as events dictate.

b) Minutes

Minutes of each Council meeting shall be made and kept documenting the information shared and decisions taken during each meeting.

c) Presiding Officer

The Council Leader shall preside at all Council meetings and may select a designee if he/she is unavailable. If the Council Leader is absent at a meeting and has not identified a designee, a majority of the Council members present shall appoint a different presiding officer for that meeting.