Washington Cybersecurity Incident Response Team Charter

Article I: Purpose, Mission, and Vision

1. **Name**: The organization shall be known as the Washington Cybersecurity Incident Response Team (CIRT).

2. **Authority**: The CIRT is established under the authority of Revised Code of Washington (RCW) 38.52.310 and administered according to Washington Administrative Code (WAC) 118-04.

3. **Purpose**: Operating under the state's Emergency Worker Program, the CIRT exists to register and preregister volunteers to provide coordinated assistance to local governments, critical infrastructure, and not-for-profit entities within Washington in mitigating and responding to cyberattacks and cybersecurity incidents. It shall leverage a pool of qualified volunteers from across the state to enhance the cyber resilience of local governments and critical infrastructure, including:

    a. Local units of government (e.g. municipalities, counties.
    b. Public sector critical infrastructure (e.g. public utilities).
    c. Cybersecurity and Infrastructure Security Agency-designated critical infrastructure owners and operators (e.g. small agribusiness, emergency fuel suppliers, healthcare facilities, etc.).
    d. School districts and private schools.
    e. Washington Universities, Technical Colleges, and similar institutions of higher education.
    f. Tribes and tribal communities located in Washington state.

4. **Mission**: CIRT's mission is to pool expertise and resources from participating public entities and private- sector partners to effectively respond to cyber incidents, minimize the impact of cyberattacks, and contribute to the overall cybersecurity risk reduction of local government and critical infrastructure entities in Washington.

5. **Vision**: The vision for CIRT is the establishment of a statewide collaborative volunteer network of cybersecurity professionals from the private and public sectors providing aid to local units of government before, during, and after cybersecurity incidents.

Article II: Membership

1. **Volunteer Basis**: Participation in the CIRT is strictly on a voluntary basis. CIRT volunteers are not employees or interns of any of the entities they assist nor of the State of Washington or any of their agencies and are not entitled to any compensation for their activities performed as a CIRT volunteer. Further, CIRT volunteers do not have any

delegated agency authority, do not have a supervisory role, and do not serve in an administrative capacity.Records held by CIRT volunteers who meet this criteria are not subject to the Public Records Act.

2. **Eligibility**: Membership in the CIRT is open to employees of all public entities and select private entities within the State of Washington who possess relevant cybersecurity skills and expertise, meet the minimum credentialling standard documented in the program handbook, have received appropriate training, are employed by a Sponsoring Organization and have passed an appropriate background check.

3. **Sponsoring Organization**: A Sponsoring Organization is an entity that supports the voluntary participation in the CIRT of an employee who performs cybersecurity functions for the entity. Sponsoring Organizations include local units of government, public utilities, health care facilities, school districts, private organizations such as managed service providers supporting cybersecurity in the public sector, financial institutions, higher education, state government agencies, law enforcement, insurance, and related organizations. A Sponsoring Organization must sign and comply with the terms of a CIRT Member Employer Agreement before its eligible employee may participate as a CIRT volunteer.
4. **Types of Memberships**: There are three types of CIRT membership. They are as follows:

    a. CIRT Affiliate: CIRT Affiliates are CIRT members who hold key positions of responsibility in private or public-sector critical infrastructure IT or cybersecurity departments but who are not General Members or Incident Responders. CIRT Affiliates are eligible for participating in general cybersecurity awareness or skills-related training activities. CIRT Affiliates are not allowed to participate in any incident response activities.

    b. General Members: CIRT General Members are eligible to participate in the statewide cybersecurity information-sharing platform. The purpose of the General Membership volunteers is to widely disseminate cybersecurity threat and vulnerability information to Organizations on relevant information to network owners within the State of Washington. General Members are allowed to participate in CIRT Collaboration Calls and participate in the Quarterly Training Program and other training opportunities. General Members are not allowed to participate in any incident response activities.

    c. Incident Responder: CIRT General Members may become Incident Responders once they have done the following:

        i. Completed and submitted a formal CIRT Membership Application, to include registration as an Emergency Worker in the State of Washington.

        ii. Submitted a signed CIRT Non-disclosure Agreement.

        iii. Obtained an InfraGard membership or TSA Known Traveler Number.

iv. Participated in one CIRT Foundations Seminar.

A CIRT member designated as a CIRT Incident Responder will be assigned a CIRT Mentor. The CIRT Membership Handbook has information about the CIRT Mentor Program.

CIRT Incident Responders must pre-register to declare their interest in providing voluntary service to support cyber (as emergency) incidents; annual re-application satisfies this requirement.

Article III: Governance

1. **Multi-Jurisdictional Collaboration**: Providing the framework for the CIRT to function is a collaborative effort among several Washington state and federal agencies including the Washington Military Department's Emergency Management Division (EMD), the federal Cybersecurity and Infrastructure Security Agency, and the Washington State Fusion Center. The agencies provide guidance, strategic and tactical recommendations to the Administration team for program development and sustainability.

2. **Leadership**: CIRT membership shall be led by the Administration personnel and CIRT Incident Response Leads. The CIRT Incident Response Leads serve the CIRT in place of a traditional Board of Directors to ensure all associated CIRT activities align with the organization's stated Mission and Vision.

3. **Administration Team**: The CIRT Administration Team is comprised of full-time EMD employees and CIRT volunteers who handle the various aspects of program functions. The day-to-day program development, strategic planning, fiscal planning, training development, and program management of the CIRT is facilitated by EMD employees, appointed by the EMD Director or designee as "authorized officials" as defined in WAC 118-04-060.

4. **CIRT Incident Response Leads**: CIRT Incident Response Leads, as members of the Leadership, assist the Administration in determining training pathways for membership progression, assessing requests for cyber incident response, vulnerability assessments, support, recovery operations, program development, and the CIRT Quarterly Training Program.

5. **Coordination**: The CIRT shall collaborate with the Washington State Fusion Center (WSFC) and other relevant state or federal agencies to ensure effective communication and coordination during cyber incidents. During active incident response operations, one or more Incident Response Leads serve as the senior cyber incident responder and establishes the appropriate course of action in collaboration with the incident network owner.

Article IV: Responsibilities

1. **Administration Team**: Specific duties and responsibilities held by the Administration team include program development, recruitment and outreach, CIRT website, monthly collaboration call, Quarterly Training Program, private-public partnership development, grants management, procurement, fiscal management, reimbursement, procedural documentation maintenance, incident response facilitation, and situation reporting to The Adjutant General and other State Agency senior leadership.
2. **CIRT Incident Response Leads**:
    a. CIRT Incident Response Leads direct the response activities of the CIRT Incident Responders mobilized in support of cyber incident operations. The Incident Response Leads have positional authority to determine whether the CIRT can support the requesting network owner.
    b. CIRT Incident Response Leads are responsible for doing the following:
        i. Determining the type of incident response needed to support the network owner.
        ii. Establishing the scope of work, remote support, on-site support, and the likely duration of support with the network owner.
        iii. Assessing when Washington National Guard partners may be needed to augment support activities.
        iv. Determining the indicators for closing the incident.
        v. Declaring an incident "closed."
    c. The CIRT Incident Responder does NOT have the authority to:
        i. Take ownership of a requestor's network or any property inherent to the requesting entity.
        ii. Request on behalf of the network owner other state resources, to include the Washington National Guard.
        iii. Act independently on behalf of the requesting network owner.
        iv. Act independently on behalf of state, local, tribal or federal law enforcement entities.
3. **Cyber Response Team (CIRT)**:
    a. Incident Response: The CIRT shall provide cybersecurity response assistance to local public- sector critical infrastructure or affiliated government entities during cyber

incidents, including but not limited to identifying and containing threats, analyzing attack vectors, and providing recommendations for recovery.

b. Prevention and Preparedness: The CIRT shall engage in proactive efforts to enhance the cybersecurity readiness of public-sector critical infrastructure and affiliated entities, including conducting training sessions, vulnerability assessments, preparedness and recovery planning, plan review, exercise development, sharing best practices, and offering guidance on cybersecurity measures.

c. Resource & Information Sharing: The CIRT shall maintain a repository of cybersecurity resources, tools, and templates that can be utilized by public-sector critical infrastructure and affiliated entities to bolster their cybersecurity preparedness. The CIRT digital communications platform (Microsoft Teams) will provide resources and information for General Members and Incident Responders.

Article V: Operations

1. **Activation**: When requested by an eligible entity, CIRT administration will request and receive a state assigned mission number issued by the State Alert and Warning Center. The CIRT shall be activated by the agreement of a CIRT Incident Response Lead and the Administration Team when a cyber incident requires assistance beyond the capabilities of the affected network owner.
2. **Volunteer Mobilization**: Upon activation, the CIRT Administration Team shall reach out to available volunteers based on the volunteers' expertise and availability to form response teams tailored to the incident's nature and severity.
3. **Coordinated Response**: The CIRT shall work closely with the network owner to provide timely and coordinated incident response, offering technical guidance, analysis, and support throughout the incident lifecycle.
4. **Incident Reporting and Closeout**: The CIRT Incident Response Lead will coordinate with an appropriate CIRT Administration Team member to provide situational awareness to appropriate state leadership on a need-to-know basis about the incident or potential impacts that may require additional resources to mitigate.

Article VI: Confidentiality, Data Privacy, Liability and Public Records Act

1. **Confidentiality**: All CIRT volunteers shall adhere to strict confidentiality standards, ensuring that sensitive information related to the incident and the affected public-sector critical infrastructure or affiliated entity is kept confidential.
2. **Data Privacy**: The CIRT shall handle any data or information obtained during incident

response in compliance with relevant laws and regulations, prioritizing the privacy and security of individuals' and organizations' data. All Incident Responders must have a signed non-disclosure agreement on file.

3. **Liability**: As registered Emergency Workers in the State of Washington, CIRT Incident Responders receive limited liability coverage. This coverage is described in RCW 38.52.180.
4. **Public Records Act**: ALL CIRT volunteers shall receive annual training from EMD on Washington's Public Records Act and other applicable laws.

Article VII: Amendments

The CIRT Administration will amend this charter as needed after consultation with key stakeholders and volunteers that will include the CIRT Incident Response Leads, Washington Emergency Management senior leadership, Department of Administration Division of Enterprise Technology senior leadership, and the Attorney General's Office.

This charter is hereby adopted on May 15, 2025, and shall remain in effect until amended or revised as outlined in Article VII.

Signed: _____ 7/18/25

Robert Ezelle, Director, Washington Emergency Management Date