Indiana Executive Council on Cybersecurity Council Charter

Last Updated: January 11, 2019

Version: 5

Table of Contents

ARTICLE 1 – BACKGROUND, NAME & PURPOSE

Section I: Background

Critical infrastructure and key resource sectors rely heavily on information technology to manage complex systems including public utilities, healthcare, telecommunications, transportation, financial services, manufacturing, education, research, and public safety. The reality of interconnectivity is that cyber risks manifest at an unprecedented pace and can pose profound effect on citizens, organizations, and industries and threaten the security and economy of Indiana. This is all the more relevant with the recent worldwide cyber-attacks.

Securing Indiana's information technology infrastructure and industrial control systems is beyond the reach of any single entity. To stay on the forefront of the cyber risk landscape, Indiana has recognized the need to take a forward-thinking approach and design initiatives that leverage whole-of-state assets.

To protect the security and economy of Indiana, Governor Holcomb's Indiana Executive Council on Cybersecurity, which is led by the Indiana Department of Homeland Security, Indiana Office of Technology, Indiana State Police, and the Indiana National Guard, was formed involving government, private-sector, military, research, and academic stakeholders to collaboratively move Indiana's cybersecurity to the Next Level.

Signed by Governor Holcomb on Jan. 9, 2017, the Council was continued through Executive Order 17-11 with the recognition that a cross-sector body of subject-matter experts is required to form an understanding of Indiana's cyber risk profile, identify priorities, establish a strategic framework of Indiana's cybersecurity initiatives, and leverage the body of talent to stay on the forefront of the cyber risk environment, especially as it gains more attention from other states, nationally, and internationally.

Section II: Name and Purpose

- The Governor has established the Indiana Executive Council on Cybersecurity (IECC or Council) to lead a statewide, public-private-sector effort to enhance the cybersecurity posture of the State of Indiana and its critical assets.

- The purpose of the Council is to (1) produce an informed overview of Indiana's cyber risks and opportunities; (2) prioritize those items by criticality, and (3) suggest and/or facilitate the implementation of programs/projects designed to achieve associated objectives.

- The Council will provide consultative direction on projects, initiatives, and programs, ensuring whole-of-state needs are met. The Council will confirm that these programs align with the unique needs and risk profiles of critical sectors throughout the state.

- The Council has been designed to accelerate cyber initiatives and ensure Indiana's cyber stakeholders have the resources and support they need to reach the Next level in cyber security.

- Per the Executive Order:
    - The Council shall develop, maintain, and execute an implementation plan for accomplishing strategic cybersecurity objectives that are specific, measurable, achievable, and relevant to the overall strategic vision, which shall be completed within an established timeframe.
    - The Council shall establish and maintain a strategic framework document that defines high-level cybersecurity goals for the State of Indiana. This framework document shall establish a strategic vision for Indiana's cybersecurity initiatives and detail how the state will:
        - Establish an effective governing structure and strategic direction;
        - Formalize strategic cybersecurity partnerships across the public and private sectors.
        - Strengthen best practices to protect information technology infrastructure;
        - Build and maintain robust statewide cyber incident response capabilities;
        - Establish processes, technology, and facilities to improve cybersecurity statewide;
        - Leverage business and economic opportunities related to information, critical infrastructure, and network security; and
        - Ensure a robust workforce and talent pipeline in fields involving cybersecurity.
    - The Council shall receive guidance from the Counter-Terrorism and Security Council and report to the Homeland Security Advisor within the Office of the Governor.

ARTICLE 2 – COUNCIL MEMBERS

Section I: Council

Per the Executive Order, the Council shall be composed of the following Voting Members who shall serve on the Council by virtue of their office or by appointment of the governor:

- A designated representative of the Governor's Office who shall also serve as the State Cybersecurity Coordinator to administer development and implementation of State cybersecurity strategy and policy.
- The Executive Director of the Indiana Department of Homeland Security, or designee.
- The Chief Information Officer of the Indiana Office of Technology, or designee.
- The Adjutant General of the Indiana National Guard, or designee.
- The Superintendent of the Indiana State Police, or designee.
- The Indiana Attorney General, or designee.
- The Chair of the Indiana Utility Regulatory Commission, or designee.
- The Secretary of Commerce of the Indiana Economic Development Corporation, or designee.
- The Commissioner of the Indiana Commission for Higher Education, or designee.
- The Commissioner of the Indiana Department of Revenue, or designee.
- The Chief Information Officer of Indiana University, or designee.
- The Chief Information Officer of Purdue University, or designee.

- One representative of a public interest organization, such as private advocacy or individual information protection.
- One (1) representative of an association representing the Information Technology Sector.
- One (1) representative of an association representing the Communications Sector.
- One (1) representative from an association representing the Defense Industrial Base Sector.
- One (1) representative from an association representing the Energy Sector.
- One (1) representative from an association representing the Financial Services Sector.
- One (1) representative from an association representing the Healthcare & Public Health Sector.
- One (1) representative from an association representing the Water & Wastewater Systems Sector.

The Council will also consist of permanent, non-voting members, as selected by the relevant federal agency:

- A Cybersecurity expert from the Indianapolis field office of the Federal Bureau of Investigation.
- Two (2) cybersecurity experts from the Indianapolis office of the United States Department of Homeland Security, as follows:
    - One (1) from the Indianapolis office of the United States Department of Homeland Security National Protection and Programs Directorate; and
    - One (1) from the Indianapolis office of the United States Secret Service.

Additional Voting Members may be appointed at the discretion of the Governor.

Section II: Classes of Members

Chairperson of the Council

- The Executive Director of the Indiana Department of Homeland Security (or designee) shall serve as **Chairperson of the Council** (the Chair)**.**
- The Chair will work in conjunction with a Core Group consisting of the Chief Information Officer of the Indiana Office of Technology, the Adjutant General of the Indiana National Guard, and the Superintendent of the Indiana State Police to strategically lead the Council.
- The Chair shall supervise and control the business, property and affairs of the Council, except as otherwise provided by law and will have final approval and signatory authority once a majority of the Core Group has approved projects overseen by the Council.
- The Chair and Core Group shall work closely with the Office of the Governor to report on and validate the processes within the Council, and escalate issues as appropriate.

- The State of Indiana may appoint a **Cybersecurity Program Director** to provide both strategy oversight, project management, and logistical support. The Cybersecurity Program Director will work closely with the Core Group, Governor's Office, and members to meet the objectives set forth by the Executive Order.

Council Members

- **Voting Members** are appointed to voice and reflect the cybersecurity issues of their sector or area of expertise.

- Voting Members may not promote their organization, company or agency over any other in the Council.

- **Non-Voting Members** have equal voice in dialogue, project proposals, and management of items brought forth to the Voting Members of the Council.

- Voting and Non-Voting Members may identify two (2) designees who may attend meetings and, if applicable, vote on their behalf.

Advisory Members

- Advisory Members may also be appointed representing both public and private sector interests. The purpose of the Advisory Members is to support Council strategy and objectives by providing subject-matter expertise and specialized, experienced insight.

- All private and academic sector Advisory Members must submit their resumes to the Cybersecurity Program Director for vetting. Resumes will be submitted through the Core Group and Governor's Office prior to being provided to the Voting and Non-Voting Members of the Council.

- Advisory Members shall be selected and approved by a majority of the Voting Members of the Council.

Contributing Members

- Pending the approval of becoming an Advisory Member, all subject matter experts will be considered Contributing Members. For long-term expertise, this is only meant as a temporary classification.

- There may be times when the Council is in need of subject-matter experts from other states or countries who provide specialized, limited guidance. These members will be considered Contributing Members.

Section III: Appointment Terms & Process

- Council Members will be appointed by the Office of the Governor for a term of one (1) year. Any representative may serve consecutive terms.

- Council Members will serve at the pleasure of the Governor of Indiana, and may be dismissed at any time.

- Any Voting, Non-Voting, or Advisory Member may be recommended in writing and with reason for removal by majority vote at a regularly scheduled meeting where the item is approved to be placed on the written agenda distributed at least two weeks ahead. The Governor's Office will have final decision-making authority over these recommended removals.

- Critical infrastructure sectors represented on the Council will be based on the most recent assessment of the State's cybersecurity landscape. Sector-specific representation may shift according to changing priorities and risk profiles.

- Council Members are expected to participate in occasional classified security briefings, and must maintain the appropriate status to be granted a temporary clearance.

- Voting, Non-Voting, and Advisory Members are required to maintain good membership standing and meet all the member terms and applicable requirements, or he or she may be removed from the council at any time.

Section IV: Membership Terms and Requirements

- All members are responsible for notifying and seeking approval from their employer to participate on the Council**.**

- All members shall continue to represent their designated organization or sector for the duration of their appointment.

- All state agencies, departments, commissions, bureaus, institutions, and entities shall cooperate to the fullest extent possible with the Executive Order.

- All members (or their proxies if applicable) shall attend at least 75 percent of all scheduled meetings in order to remain in good standing. Members who fail to meet this expectation will be reported to the Chair, Core Group, and Office of the Governor and may be removed from the Council.

- All members who wish to withdraw their membership may do so at any time by submitting a written request to the Chair and Cybersecurity Program Director.

- All members are required to sign and submit a Non-Disclosure Agreement before attending any executive session.

- All members are required to complete Inspector General Ethics Training and applicable forms (e.g. disclosures) in a timely fashion and follow the laws set forth in statute.

- All members shall do their best to avoid any look of impropriety regarding their membership and the Council.

- All private sector members are required to be an InfraGard member and must submit timely proof of membership.

- All public and academic members are strongly encouraged to be an InfraGard member. If he or she is a member, membership proof is required to be submitted.

- All members must have access and agree to use the software platform for central repository and project management selected for the Council by the Cybersecurity Program Director.

- All members must serve in a capacity in at least one of the committees or working groups.

- All members will be required to complete a *Committee and Work Group Form* and submit it to the Cybersecurity Program Director for consideration.

- All members must comply with the charters and guidelines set forth by the Council, committees, and/or working groups in which they are involved.

Section V: Member Expenses

- Participation in the Council is entirely voluntary, and expenses for travel, per diem, etc. will not be remunerated at this time.

ARTICLE 3 – COUNCIL MEETINGS

Section I: Schedule & Process

- The Council Meeting schedule and agendas are collectively set by the Chair, Core Group, Governor's Office, and Cybersecurity Program Director.

- Meetings shall generally be held on a quarterly basis or as needed per the strategic plan deadlines and approvals.

- A special or emergency Council meeting may be called in the case of pertaining events. This may be done at the suggestion of a Council Member(s) or the Chair at a permitting facility.

Section II: Announcement of Meetings

- The Council shall be subject to the requirements as well as the security and confidentiality exceptions under the Indiana Open Door Law, per the Executive Order.

- Members will be notified at each meeting of the next meeting time, place, and date, and will be notified in writing at least four weeks in advance of such meetings with a verified date, time, and place. All materials subject to vote and a draft agenda will be provided to Voting and Non-Voting Members at least two weeks prior to the scheduled meeting.

- The public will be notified of Council meetings by notices issued by the Indiana Department of Homeland Security, in the manner prescribed by law.

- Executive sessions exclusive to Council Members may be scheduled at the discretion of the Chair or designee.

- The Council herby adopts a policy so that the committees and working groups may conduct meetings using means of electronic communication per IC 5-14-1.5-3.6.

Section III: Location of Meetings

- Council meetings shall be held in the Indiana Government Center's Conference Center, 302 West Washington Street, Indianapolis, Indiana 46204, or as otherwise determined by the Chair.

- Exceptions may be permitted for off-site meetings at the suggestion of Council Member(s) and at the discretion of the Chair.

- Attending meetings by conference call or Internet usage is prohibited. Council Members who cannot attend may have a proxy attend in their stead.

Section IV: Quorum of Members for Meetings

- A quorum of 85 percent of the Voting and Non-Voting Council Members is required for the conduct of business and consists of the presence of a majority of its members.

Section V: Conduct of Meetings

- Council meetings will be conducted according to Robert's Rules of Order, and Council business according to the provisions of the Indiana Open Door Law, the Indiana Public Records Law, and the Indiana Administrative Orders and Procedures Act.

- A vote may be held to approve Council activities or statewide strategic projects, documents, and requests to the Governor's Office or General Assembly.

- Any matter to be voted on will take the form of a resolution or motion. A simple majority of the Voting Members in attendance at a Council meeting must vote affirmatively, for the adoption of any resolution.

- Each Voting Member will have one vote.

- A Council Member may vote for or against a resolution, or may abstain from voting.

- All Voting Members of the Council shall have equal voting rights.

- Votes must be cast in person. Council Members who cannot attend may have one of their pre-approved designees vote on their behalf.

Section VI: Delegation of Authority

- In the absence of the Director, Council meetings will be conducted by the Cybersecurity Program Director or Chair's designee.

- The Council Chair may delegate in writing at his or her discretion his or her powers and duties consistent with other provisions of the Charter.

- Each Council Member may provide in writing up to two (2) designees with full voting rights to represent such organizational head in his/her absence from Council meetings.

Section VII: Conflict of Interest

- Whenever a Voting Member has a financial interest in a matter coming before the Council, the person shall a.) fully disclose the nature of the interest and b.) withdraw from a voting process.

- The meeting minutes at which such votes are taken shall record such disclosure, abstention and rationale for approval.

ARTICLE 4 – COUNCIL DUTIES

Section I: Cyber Projects and Events

- Council Members representing state departments/agencies are expected to leverage the expertise provided by the Council and submit statewide, cross-sector, or significant cybersecurity projects and/or events to the Council for review and input, except in instances in which doing so would be in violation of law or policy, or in which doing so could jeopardize the event or project.

- Council Members representing the private and academic sector are strongly encouraged to leverage the expertise provided by the Council and request the participation or feedback of all Council Members on statewide or cross-sector cybersecurity projects and/or events.

- In an effort to cross-promote cyber events in Indiana, members are encouraged to submit cyber events to the Cybersecurity Program Director to list on www.in.gov/cybersecurity at least six weeks prior to the event. Once a month, a notification will be sent to subscribers and all Council members.

- Agency heads or project managers may submit their project proposals to the Cybersecurity Program Director at least six weeks before the requested meeting date.

- Council Members may suggest changes to project content submitted to the Council based on their subject-matter expertise; suggestions will be non-binding unless the matter requested to be escalated to a vote by the responsible agency head or project manager.

Section II: Committees and Working Groups

- All members must serve in a capacity in at least one of the committees or working groups:
  - Government Service Committee
  - Finance Committee
  - Energy Committee
  - Water and Wastewater Committee
  - Communications Committee
  - Healthcare Committee
  - Defense Industrial Committee
  - Elections Committee
  - Economic Development Committee
  - Workforce Development Committee
  - Personal Identifiable Information Working Group
  - Public Awareness and Training Working Group
  - Emergency Services and Exercise Working Group
  - Cyber Sharing Working Group
  - Policy Working Group
  - Cyber Pre- and Post- Incident Working Group
  - Legal and Insurance Working Group
  - Local Government Working Group
  - Cyber Summit Working Group
  - Strategic Resource Working Group

- All members must comply with the charters and guidelines set forth by the Council, committees, and/or working groups in which they are involved.

- Membership of each committee and workgroup consist of:
  - Chairs
  - Co-Chairs
  - Full-time Members
  - As-needed Members

- All members will be required to complete a *Committee and Work Group Form* and submit it to the Cybersecurity Program Director. Choices will be strongly considered, but not guaranteed. No one person can participate in more than three committees or working groups. This is to ensure that all committees and working groups are as cross-functional and diverse in its expertise as possible.

- All Committee and Working Groups will provide the Cybersecurity Program Director an update quarterly, per the details of the committee's charter or working group guidelines.

Section III: Deadlines

All members of the Council shall meet all established deadlines of items for review, deliverables, and strategy. If a deadline will not be met, member is responsible for notifying the Cybersecurity Program Director with the reason why the deadline will be missed and the expected completion date.

Section IV: Document Submissions

Sharing and Editing of Documents

- For the purposes of the electronic file sharing and a central repository, all members will be required to sign up and use Syncplicity (https://www.syncplicity.com/register/personal). If a member is a State of Indiana employee, he or she will receive an email from the Indiana Office of Technology to set up their state account. Once signed up, each member will be invited by the Cybersecurity Program Director to join his or her relative folders.

Repository of Documents

- The Indiana Department of Homeland Security (IDHS), 302 West Washington Street, Room E238, Indianapolis, Indiana 46204 will be the repository for all documents submitted to the Council pursuant to the provisions of federal or state law.

Availability of Documents to the Public

- Public records will be available for examination by the public during the hours of 8:30 am and 4:30 pm, Monday through Friday.

Council Records

- All records of general meetings, including meeting agendas and minutes, will be available for inspection and copying by any person at 302 West Washington Street, Room E238, Indianapolis, Indiana 46204.

Section V: Media Request

- If a member is contacted by the media for an issue related to the IECC, please direct them to the IDHS Office of Public Affairs at PIO@dhs.in.gov or 317-234-6713.

Section VI: Receipt of Sensitive Information

- The Council may receive sensitive security information from the Indiana Department of Homeland Security, Indiana Office of Technology, or the Indiana Army National Guard. This information shall remain for official use only, and Council Members are expected to abide by handling instructions.

- The Council may receive sensitive law enforcement information from the State Police Department, the Federal Bureau of Investigation, or other federal, state, or local law enforcement agencies. This information shall not be released to the news media or others without a need to know.

- Council Members who release such information to external parties without prior approval are subject to immediate dismissal from the Council.

ARTICLE 5 – ADOPTION/AMENDMENT OF COUNCIL CHARTER

- A majority of Council Members is required to adopt the Council's Charter.
- Once approved, the Council Charter will be reviewed every year.
- The Charter may be amended by majority vote at a regularly scheduled Council meeting.

ARTICLE 6 – NON-EXCLUSION PROVISION

- Nothing in this Charter is to be construed as excluding or contravening any additional provisions of federal or state law that are not explicitly or implicitly referred to within this Charter.

ARTICLE 7 – CHARTER ADOPTION & SIGNING

Upon their adoption by the Council, a copy of this Charter will be signed and dated by the Chair, Core Group, and the Cybersecurity Program Director of the Council and will be available for inspection by the public at 302 W. Washington Street, Room E238, Indianapolis, Indiana.