STATE OF INDIANA

EXECUTIVE DEPARTMENT
INDIANAPOLIS

EXECUTIVE ORDER 26-19

FOR: COORDINATING THE NEXT PHASE OF WHOLE OF GOVERNMENT CYBERSECURITY FOR THE STATE OF INDIANA

TO ALL WHOM THESE PRESENTS MAY COME, GREETINGS.

WHEREAS, all modern life is dependent upon information technology and operational technology to provide services that enable our daily activities, facilitate conducting business, and provide safe and healthy communities;

WHEREAS, such systems are susceptible to cyber attacks by financially motivated criminals, ideological hacktivists, foreign nation states, and other malicious actors to steal, delete, or compromise sensitive data and disrupt or deny system operations;

WHEREAS, the federal Cybersecurity and Infrastructure Security Agency describes "critical infrastructure" as 16 sectors that are, "part of a complex, interconnected ecosystem and any threat to these sectors could have potentially debilitating national security, economic, and public health or safety consequences";

WHEREAS, a cyberattack is one of the greatest threats to Indiana, posing personal, professional, and financial risks to the citizens of the State of Indiana and threatening the security and economy of our State;

WHEREAS, the Indiana Executive Council on Cybersecurity ("IECC"), the State's public and private sector cybersecurity working group sunsets on July 1, 2026;

WHEREAS, the IECC has done tremendous work and laid the groundwork for the next phase of cybersecurity in Indiana;

WHEREAS, the State's commitment to a robust cybersecurity should be institutionalized within an existing State agency;

WHEREAS, the Indiana Department of Homeland Security ("IDHS") is statutorily required by IC 10-14-2-4 to, "serve as the coordinating agency for all state efforts for preparedness for, response to, mitigation of, and recovery from emergencies and disasters"; and

WHEREAS, IC 10-14-3-1 provides that a "technology emergency" is a "disaster."

NOW, THEREFORE, I, MIKE BRAUN, by virtue of the authority vested in me as the Governor of the State of Indiana, do hereby order the following:

1. IDHS shall establish an Office of Cybersecurity ("Office") within IDHS to serve as the lead coordinating entity for cybersecurity activities in order to protect the security and economy of the State.
2. The Office shall operate in partnership with the following entities to bring a "whole of government" approach to address cybersecurity risks in the State that pose the greatest threats to Hoosier's life and safety:
    a. The Indiana Office of Technology;
    b. The Indiana National Guard; and
    c. The Indiana State Police.

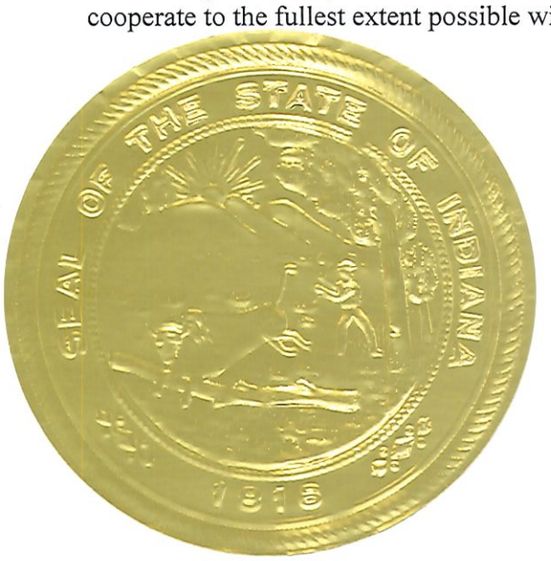
3. The Office shall:
    a. Work with applicable state agencies to clearly define each agencies' roles and responsibilities, within current statutory authority, regarding prevention of and response to a cybersecurity incident affecting State government, local government, or critical infrastructure in Indiana;
    b. Streamline and coordinate information sharing regarding cybersecurity incidents with appropriate local, state, and federal partners;
    c. Proactively engage with critical infrastructure owners and operators to establish lines of communication, increase information sharing, and increase Indiana's cybersecurity resiliency;
    d. Identify ways to appropriately share cyber threat intelligence with governmental entities and public or private sector organizations;
    e. Maintain the Indiana Cybersecurity Hub and its resources regarding best practices for cybersecurity;
    f. Make recommendations as needed to the Governor and Indiana General Assembly regarding executive actions or legislative actions that may be needed to enhance the State's ability to deter, detect, respond to, and recover from cybersecurity attacks;
    g. Partner with institutions of higher education and other public and private sector organizations to increase the state's cyber resiliency.

4. In addition to the entities described in paragraph 2, the Office may collaborate with:
    a. The Indiana Attorney General;
    b. The Indiana Utility Regulatory Commission;
    c. The Indiana Department of Environmental Management;
    d. Suitable federal partners, including the Federal Bureau of Investigation and the Cybersecurity and Infrastructure Security Agency;
    e. Suitable information sharing and analysis centers;
    f. Owners or operators of critical infrastructure in Indiana;
    g. Local government officials;
    h. Cybersecurity or information technology professionals, or equivalent individuals from private or non-profit entities;
    i. Educational institutes; or
    j. Any person or entity the Office believes is necessary to carry out its duties.

5. The Office shall host periodic public cybersecurity summits to inform industry of its current actions, solicit feedback, and brief on current cybersecurity threats or trends.

6. The Office shall brief the Governor's Security Council established in IC 10-19-8.1 upon request of the Council.

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



IN TESTIMONY WHEREOF,
I, Mike Braun, have hereunto set my hand and caused to be affixed the Great Seal of the State of Indiana on this 24th day of July, 2026.

Mike Braun
Governor of Indiana

DIEGO MORALES

ATTEST: Diego Morales | Secretary of State