Effective 5/1/2024

63A-16-1102 Utah Cyber Center -- Creation -- Duties.

(1)

(a) There is created within the division the Utah Cyber Center.

(b) The chief information security officer appointed under Section 63A-16-210 shall serve as the director of the Cyber Center.

(2) The division shall operate the Cyber Center in partnership with the following entities within the Department of Public Safety created in Section 53-1-103:

(a) the Statewide Information and Analysis Center;

(b) the State Bureau of Investigation created in Section 53-10-301; and

(c) the Division of Emergency Management created in Section 53-2a-103.

(3) In addition to the entities described in Subsection (3), the Cyber Center shall collaborate with:

(a) the Cybersecurity Commission created in Section 63C-27-201;

(b) the Office of the Attorney General;

(c) the Utah Education and Telehealth Network created in Section 53B-17-105;

(d) appropriate federal partners, including the Federal Bureau of Investigation and the Cybersecurity and Infrastructure Security Agency;

(e) appropriate information sharing and analysis centers;

(f) information technology directors, cybersecurity professionals, or equivalent individuals representing political subdivisions in the state; and

(g) any other person the division believes is necessary to carry out the duties described in Subsection (4).

(4) The Cyber Center shall, within legislative appropriations:

(a) by June 30, 2024, develop a statewide strategic cybersecurity plan for governmental entities;

(b) with respect to executive branch agencies:

(i) identify, analyze, and, when appropriate, mitigate cyber threats and vulnerabilities;

(ii) coordinate cybersecurity resilience planning;

(iii) provide cybersecurity incident response capabilities; and

(iv) recommend to the division standards, policies, or procedures to increase the cyber resilience of executive branch agencies individually or collectively;

(c) at the request of a governmental entity, coordinate cybersecurity incident response for a data breach affecting the governmental entity in accordance with Section 63A-19-405;

(d) promote cybersecurity best practices;

(e) share cyber threat intelligence with governmental entities and, through the Statewide Information and Analysis Center, with other public and private sector organizations;

(f) serve as the state cybersecurity incident response repository to receive reports of breaches of system security, including notification or disclosure under Section 13-44-202 and data breaches under Section 63A-16-1103;

(g) develop incident response plans to coordinate federal, state, local, and private sector activities and manage the risks associated with an attack or malfunction of critical information technology systems within the state;

(h) coordinate, develop, and share best practices for cybersecurity resilience in the state;

(i) identify sources of funding to make cybersecurity improvements throughout the state;

(j) develop a sharing platform to provide resources based on information, recommendations, and best practices; and

(k) partner with institutions of higher education and other public and private sector organizations to increase the state's cyber resilience.

Renumbered and Amended by Chapter 426, 2024 General Session