Protecting the Water Sector’s Critical Infrastructure Information

Analysis of State Laws

American Water Works Association
Dedicated to the World’s Most Important Resource®
Acknowledgements

The research for this report was supported by policy interns in AWWA's Government Affairs Office in Washington, DC, including Gabriela Rossner and Erin Ress and managed by Kevin Morley, AWWA Federal Relations Manager.

Disclaimer

This report includes excerpts of statutory text addressing the protections provided to information that may be included in a risk and resilience assessment and/or emergency response plan prepared by a community water system in compliance with §2013 of Americas Water Infrastructure Act of 2018. This report is provided for reference purposes only and does not represent an official legal opinion. Legal counsel should be consulted when exercising these information protections.
SUMMARY:

America’s Water Infrastructure Act (AWIA) of 2018 requires community water systems that serve 3,300 or more persons to 1) conduct a risk and resilience assessment (RRA) and 2) prepare or revise an emergency response plan (ERP). In recognition of the security sensitive information developed by state and local entities, many states have taken steps to exempt this information from public release. Thirty-four states currently have disclosure exemption laws that specifically address the type of information a utility would be required to develop and prepare in compliance with AWIA. The remaining states have some protections that may, or may not, apply to critical infrastructure information. This report is a review and summary of the protections available for the information developed by a water utility per AWIA at the state level.

The AWIA RRAs must evaluate risk to the water system from malevolent threats and natural hazards. The ERPs must include strategies to improve the resilience of the system, including the physical security and cybersecurity of the system. The utility must then certify to the US Environmental Protection Agency (EPA) that the RRA and ERP have been completed based on the statutory deadline in Table 1 and every 5 years thereafter.

<table>
<thead>
<tr>
<th>Community Water System (population served) *</th>
<th>Certify RRA prior to:</th>
<th>Certify ERP within 6 months of RRA but not later than</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt;100,000</td>
<td>March 31, 2020</td>
<td>September 30, 2020</td>
</tr>
<tr>
<td>50,000 – 99,999</td>
<td>December 31, 2020</td>
<td>June 30, 2021</td>
</tr>
<tr>
<td>3,300 – 49,999</td>
<td>June 30, 2021</td>
<td>December 30, 2021</td>
</tr>
</tbody>
</table>

* Wholesale systems must use the total population of all systems served.

The term critical infrastructure is defined in §1016(e) of the Patriot Act of 2001 (42 U.S.C. 5195c(e)) as “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters”. This is the legal definition from which federal and state laws derive their characterization of critical infrastructure. Under this definition, water and wastewater systems are designated as critical infrastructure per Presidential Policy Directive 21: Critical Infrastructure Security and Resilience.1

At the federal level, the Freedom of Information Act (FOIA) provides a mechanism to request and/or share government information with the public. While an informed citizenry is crucial to a thriving democracy, the wide release of security sensitive information related to critical infrastructure systems, such as water and wastewater systems, can create a public safety and security risk.

In the post-9/11 and Hurricane Katrina era, water utilities are aware of the physical, cyber, and natural threats that may impact their operations. As such, the information contained in the mandated RRA and ERP under AWIA is considered security sensitive. In recognition of this

1 PPD-21 (Obama) supersedes HSPD-7 (Bush), which was preceded by PDD-63 (Clinton).
sensitivity, AWIA protects any information submitted to the EPA from disclosure at the federal level as follows:

Protection from disclosure. Information submitted to the Administrator of the Environmental Protection Agency pursuant to section 1433 of the Safe Drinking Water Act, as in effect on the day before the date of enactment of America’s Water Infrastructure Act of 2018, shall be protected from disclosure in accordance with the provisions of such section as in effect on such day.

AWIA section 2013 requires a utility to certify to EPA that the RRA and ERP have been completed. The utility is not required to submit the actual RRA or ERP to EPA, therefore they are not explicitly protected from disclosure under the federal statute. Protection of the information they contain defaults to state law regarding public disclosure requirements. As such, an information request could make these security sensitive plans public until such time that the state law is changed or amended if not covered by existing exclusions.

Many states have enacted laws to exempt security related infrastructure plans from public release. These exemptions differ by state, and the level of protection afforded specifically to water infrastructure information is variable. This report summarizes, to the best of our knowledge, the status of current state laws and statutes regarding protections for security sensitive information that may be created, produced, and stored by a water utility. Legal counsel should be consulted for the most current statutory reading.

For this review, each state has been categorized as Explicit, Moderate, or Unspecified based on the level of protection afforded by the state law.

- **Explicit** is applied when the state law directly includes exemption criteria for information that is associated with public safety, risk assessments, or emergency plans prepared by critical infrastructure, and in some instances specifically naming drinking water systems. There are 34 states included in this category.

- **Moderate** is applied when the state law provides protection to some portion of the information required by AWIA but may not clearly capture all elements. There are 14 states in this category.

- **Unspecified** is applied when the state law provides no explicit protection for information that may be included in RRA and ERP. This is also applied when the state law defers to protections afforded to information by federal statute. Of note is that existing federal law does not protect the plans from release at the state level. There are 8 states in this category.
<table>
<thead>
<tr>
<th>State</th>
<th>Statutory Citation</th>
<th>Criteria</th>
<th>Characterization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alabama</td>
<td>Ala. Code §36-12-40</td>
<td>Critical infrastructure</td>
<td>Explicit</td>
</tr>
<tr>
<td>Alaska</td>
<td>Alaska Stat. §40.25.120(a)(10)</td>
<td>Infrastructure</td>
<td>Moderate</td>
</tr>
<tr>
<td>American Samoa</td>
<td>A.S.A.C §4.1105</td>
<td>Public record</td>
<td>Unspecified</td>
</tr>
<tr>
<td>California</td>
<td>Cal. Gov. Code §6254(aa)-(ab)</td>
<td>Critical infrastructure</td>
<td>Explicit</td>
</tr>
<tr>
<td>Delaware</td>
<td>29 Del. Code Ann. §10002(17A)</td>
<td>Water systems’ security</td>
<td>Explicit</td>
</tr>
<tr>
<td>District of Columbia</td>
<td>D.C. Statute §2-534(10)</td>
<td>Response plan/ vulnerability assessment</td>
<td>Explicit</td>
</tr>
<tr>
<td>Florida</td>
<td>Fla. Stat. §119.071(3)</td>
<td>Response plan, sunsets 2023</td>
<td>Moderate</td>
</tr>
<tr>
<td>Guam</td>
<td>5 GCA §10108</td>
<td>Security procedures</td>
<td>Moderate</td>
</tr>
<tr>
<td>Hawaii</td>
<td>Hawaii Rev. Stat. §92F-13</td>
<td>Existing federal law</td>
<td>Unspecified</td>
</tr>
<tr>
<td>Idaho</td>
<td>Idaho Code §74-105(4)(b)</td>
<td>Vulnerability assessment</td>
<td>Explicit</td>
</tr>
<tr>
<td>Illinois</td>
<td>5 ILCS 140/7(1)(k,o,v)</td>
<td>Vulnerability assessment, security and response plans</td>
<td>Explicit</td>
</tr>
<tr>
<td>Indiana</td>
<td>Ind. Code 5-14-3-4(4)(b)(19)</td>
<td>Public safety, water and wastewater</td>
<td>Explicit</td>
</tr>
<tr>
<td>Iowa</td>
<td>Iowa Code §22.7(45),(50),(71)</td>
<td>Critical infrastructure, vulnerability, cyber</td>
<td>Explicit</td>
</tr>
<tr>
<td>Kentucky</td>
<td>Ky. Rev. Stat. §61.878(m)</td>
<td>Critical infrastructure</td>
<td>Explicit</td>
</tr>
<tr>
<td>Louisiana</td>
<td>La. Rev. Stat. §44.3(A)(3), §44.3.1</td>
<td>Vulnerability assessments</td>
<td>Explicit</td>
</tr>
<tr>
<td>Maryland</td>
<td>MD Gen Provisions Code § 4-352</td>
<td>Response plans, water systems</td>
<td>Explicit</td>
</tr>
<tr>
<td>Massachusetts</td>
<td>Mass. Gen. L. Ch. 4, §7.26(n)</td>
<td>Risk assessments, infrastructure</td>
<td>Explicit</td>
</tr>
<tr>
<td>Michigan</td>
<td>Mich. Comp. Laws §15.243(1,y)</td>
<td>Public safety, public water supply</td>
<td>Explicit</td>
</tr>
<tr>
<td>Minnesota</td>
<td>Minn. Stat. Ann. §13.03 &amp; §13.06</td>
<td>Data Classification</td>
<td>Unspecified</td>
</tr>
<tr>
<td>Mississippi</td>
<td>Miss. Code Ann. §25-61-5 and §25-61-11.2</td>
<td>Information technology</td>
<td>Moderate</td>
</tr>
<tr>
<td>Missouri</td>
<td>Mo. Rev. Stat §610.021(18-21)</td>
<td>Public safety, infrastructure</td>
<td>Explicit</td>
</tr>
<tr>
<td>Montana</td>
<td>Mont. Code Ann. §2-6-1003</td>
<td>Public safety</td>
<td>Moderate</td>
</tr>
<tr>
<td>Nebraska</td>
<td>Neb. Rev. Stat. §84-712.05(8)</td>
<td>Vulnerability assessments</td>
<td>Explicit</td>
</tr>
<tr>
<td>State</td>
<td>Statutory Citation</td>
<td>Criteria</td>
<td>Characterization</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Nevada</td>
<td>NRS 239C.210&lt;br&gt;NRS 239C.250&lt;br&gt;NRS 239C.270&lt;br&gt;N.H. Rev Stat §91-A:5(VI)</td>
<td>Vulnerability assessment, Critical infrastructure</td>
<td>Explicit</td>
</tr>
<tr>
<td>New Mexico</td>
<td>N.M. Stat. Ann. §14-2-1(G)</td>
<td>Risk assessments, emergency plans</td>
<td>Explicit</td>
</tr>
<tr>
<td>New York</td>
<td>N.Y. PH Law Sec. 1125(B)&lt;br&gt;N.Y. Pub. Off. Law §47-6-87(2a.f.)</td>
<td>Water infrastructure reports, public safety</td>
<td>Explicit</td>
</tr>
<tr>
<td>North Carolina</td>
<td>N.C. Gen. Stat. §132-1.7</td>
<td>Risk assessments, emergency preparedness</td>
<td>Explicit</td>
</tr>
<tr>
<td>North Dakota</td>
<td>N.D. Cent. Code §44-04-24</td>
<td>Critical infrastructure security plan</td>
<td>Explicit</td>
</tr>
<tr>
<td>Northern Mariana Islands</td>
<td>1 CMC §9917, §9918</td>
<td>Public records</td>
<td>Unspecified</td>
</tr>
<tr>
<td>Ohio</td>
<td>Ohio Rev. Code Ann 149-433</td>
<td>Risk assessment, emergency management plan</td>
<td>Explicit</td>
</tr>
<tr>
<td>Oregon</td>
<td>Or. Rev. Stat. §192.335(33)</td>
<td>Water security</td>
<td>Moderate</td>
</tr>
<tr>
<td>Pennsylvania</td>
<td>Pa. Stat. § 67.708(b)</td>
<td>Physical security, critical systems</td>
<td>Explicit</td>
</tr>
<tr>
<td>Puerto Rico</td>
<td>32 L.P.R.A. § 178</td>
<td>Existing laws</td>
<td>Unspecified</td>
</tr>
<tr>
<td>South Carolina</td>
<td>S.C. Code Ann. 30-4</td>
<td>Existing laws</td>
<td>Moderate</td>
</tr>
<tr>
<td>South Dakota</td>
<td>S.D. Codified Law Ann 1-27-1.5</td>
<td>Existing laws</td>
<td>Moderate</td>
</tr>
<tr>
<td>Texas</td>
<td>Tex Code Ann. Sec. 552.139</td>
<td>Exemption only for computer systems, continuity of operations</td>
<td>Moderate</td>
</tr>
<tr>
<td>US Virgin Islands</td>
<td>3 VIC §881(g)(14)</td>
<td>Homeland Security</td>
<td>Moderate</td>
</tr>
<tr>
<td>Utah</td>
<td>Utah Code Ann. §63G-2-106</td>
<td>Existing laws</td>
<td>Moderate</td>
</tr>
<tr>
<td>Virginia</td>
<td>Va. Code §2.2-3705.2(14)</td>
<td>Risk assessment, critical infrastructure</td>
<td>Explicit</td>
</tr>
<tr>
<td>Washington</td>
<td>Wash. Rev. Code §42.56.420</td>
<td>Public safety</td>
<td>Moderate</td>
</tr>
<tr>
<td>West Virginia</td>
<td>W.Va. Code Sec. §29B-1-4</td>
<td>Risk assessment, utilities</td>
<td>Explicit</td>
</tr>
<tr>
<td>Wisconsin</td>
<td>Wis. Stat. §19-35(1)(a)</td>
<td>Existing laws</td>
<td>Unspecified</td>
</tr>
<tr>
<td>Wyoming</td>
<td>Wyo. Stat. §16-4-203(b)(vi)</td>
<td>Vulnerability assessments, emergency procedures</td>
<td>Explicit</td>
</tr>
</tbody>
</table>
Level of Protection by State
Statutory Text by State or Territory

This section provides excerpts of the relevant statutory text addressing the protections provided for information that may be included in a risk and resilience assessment and/or emergency response plan prepared by a community water system in compliance with §2013 of America's Water Infrastructure Act of 2018. This report is provided for reference purposes only and does not represent an official legal opinion. Legal counsel should be consulted when exercising these information protections.

Alabama: Ala. Code §36-12-40

Rights of citizens to inspect and copy public writings; exceptions.

Every citizen has a right to inspect and take a copy of any public writing of this state, except as otherwise expressly provided by statute. Notwithstanding the foregoing, records concerning security plans, procedures, assessments, measures, or systems, and any other records relating to, or having an impact upon, the security or safety of persons, structures, facilities, or other infrastructures, including without limitation information concerning critical infrastructure (as defined at 42 U.S.C. §5195c(e) as amended) and critical energy infrastructure information (as defined at 18 C.F.R. §388.113(c)(1) as amended) the public disclosure of which could reasonably be expected to be detrimental to the public safety or welfare, and records the disclosure of which would otherwise be detrimental to the best interests of the public shall be exempted from this section. Any public officer who receives a request for records that may appear to relate to critical infrastructure or critical energy infrastructure information, shall notify the owner of such infrastructure in writing of the request and provide the owner an opportunity to comment on the request and on the threats to public safety or welfare that could reasonably be expected from public disclosure on the records.

Alaska: Alaska Stat. §40.25.120(a)(10)

Public Records; Exceptions; Certified Copies.

(a) Every person has a right to inspect a public record in the state, including public records in recorders’ offices, except:

(10) records or information pertaining to a plan, program, or procedures for establishing, maintaining, or restoring security in the state, or to a detailed description or evaluation of systems, facilities, or infrastructure in the state, but only to the extent that the production of the records or information

(A) could reasonably be expected to interfere with the implementation or enforcement of the security plan, program, or procedures;

(B) would disclose confidential guidelines for investigations or enforcement and the disclosure could reasonably be expected to risk circumvention of the law; or

(C) could reasonably be expected to endanger the life or physical safety of an individual or to present a real and substantial risk to the public health and welfare;
American Samoa: **A.S.A.C §4.1105**

4.1105 Records to be public—Inspection.

All books of registry, the records contained in them and the indexes of their contents shall be public records and open to the inspection of the public at the registration office, in the presence of the territorial registrar or one of his assistants during office hours.


Nothing in this chapter requires the disclosure of a risk assessment that is performed by or on behalf of a federal agency to evaluate critical energy, water or telecommunications infrastructure to determine its vulnerability to sabotage or attack.


Drinking water system security vulnerability assessments that are submitted to the United States environmental protection agency, pursuant to Public Law 107-188, are exempt from disclosure under this chapter and title 39, chapter 1.


(b) It is the specific intent of this section that the following shall not be deemed to be made open to the public under the provisions of this chapter

16) Vulnerability assessments submitted by a public water system on or before June 30, 2004, to the Administrator of the United States Environmental Protection Agency for a period of ten (10) years from the date of submission;

18) (A) Records, including analyses, investigations, studies, reports, recommendations, requests for proposals, drawings, diagrams, blueprints, and plans, containing information relating to security for any public water system.

(B) The records shall include:

(i) Risk and vulnerability assessments;

(ii) Plans and proposals for preventing and mitigating security risks;

(iii) Emergency response and recovery records;

(iv) Security plans and procedures; and

(v) Any other records containing information that if disclosed might jeopardize or compromise efforts to secure and protect the public water system.
California: Cal. Gov. Code §6254(aa)-(ab)
Except as provided in Sections 6254.7 and 6254.13, this chapter does not require the disclosure of any of the following records:

(aa) A document prepared by or for a state or local agency that assesses its vulnerability to terrorist attack or other criminal acts intended to disrupt the public agency’s operations and that is for distribution or consideration in a closed session.

(ab) Critical infrastructure information, as defined in Section 131(3) of Title 6 of the United States Code, that is voluntarily submitted to the Office of Emergency Services for use by that office, including the identity of the person who or entity that voluntarily submitted the information. As used in this subdivision, “voluntarily submitted” means submitted in the absence of the office exercising any legal authority to compel access to or submission of critical infrastructure information. This subdivision shall not affect the status of information in the possession of any other state or local governmental agency.

(2)(a) The custodian may deny the right of inspection of the following records, unless otherwise provided by law, on the ground that disclosure to the applicant would be contrary to the public interest:

(VIII)(A) Specialized details of either security arrangements or investigations or the physical and cyber assets of critical infrastructure, including the specific engineering, vulnerability, detailed design information, protective measures, emergency response plans, or system operational data of such assets that would be useful to a person in planning an attack on critical infrastructure but that does not simply provide the general location of such infrastructure. Nothing in this subsection (2)(a)(VIII) prohibits the custodian from transferring records containing specialized details of either security arrangements or investigations or the physical and cyber assets of critical infrastructure to the division of homeland security and emergency management in the department of public safety, the governing body of any city, county, city and county, or other political subdivision of the state, or any federal, state, or local law enforcement agency; except that the custodian shall not transfer any record received from a nongovernmental entity without the prior written consent of the entity unless such information is already publicly available.

(b) Nothing in the Freedom of Information Act shall be construed to require disclosure of:

(19) Records when there are reasonable grounds to believe disclosure may result in a safety risk, including the risk of harm to any person, any government-owned or leased institution or facility or any fixture or appurtenance and equipment attached to, or contained in, such institution or facility, except that such records shall be disclosed to a law enforcement agency upon the request of the law enforcement agency. Such reasonable grounds shall be determined (A) (i) by the Commissioner of Administrative Services, after consultation with the chief executive officer of an executive branch state agency, with respect to records concerning such agency; and (ii) by the Commissioner of Emergency Services and Public Protection, after consultation with the chief executive officer of a municipal, district or regional agency, with respect to records concerning such agency; (B) by the Chief Court Administrator with respect to records concerning the Judicial Department; and (C) by the executive director of the Joint Committee on Legislative Management, with respect to records concerning the Legislative Department. As used in this section, “government-owned or leased institution or facility” includes, but is not limited to, an institution or facility owned or leased by a public service company, as defined in section 16-1, a certified telecommunications provider, as defined in section 16-1, a water company, as defined in section 25-32a, or a municipal utility that furnishes electric, gas or water service, but does not include an institution or facility owned or leased by the federal government, and “chief executive officer” includes, but is not limited to, an agency head, department head, executive director or chief executive officer. Such records include, but are not limited to:

(i) Security manuals or reports;

(ii) Engineering and architectural drawings of government-owned or leased institutions or facilities;

(iii) Operational specifications of security systems utilized at any government-owned or leased institution or facility, except that a general description of any such security system and the cost and quality of such system, may be disclosed;

(iv) Training manuals prepared for government-owned or leased institutions or facilities that describe, in any manner, security procedures, emergency plans or security equipment;

(v) Internal security audits of government-owned or leased institutions or facilities;

(vi) Minutes or records of meetings, or portions of such minutes or records, that contain or reveal information relating to security or other records otherwise exempt from disclosure under this subdivision;

(vii) Logs or other documents that contain information on the movement or assignment of security personnel;

(viii) Emergency plans and emergency preparedness, response, recovery and mitigation plans, including plans provided by a person to a state agency or a local emergency management agency or official; and
(d) Whenever a public agency, except the Judicial Department or Legislative Department, receives a request from any person for disclosure of any records described in subdivision (19) of subsection (b) of this section under the Freedom of Information Act, the public agency shall promptly notify the Commissioner of Administrative Services or the Commissioner of Emergency Services and Public Protection, as applicable, of such request, in the manner prescribed by such commissioner, before complying with the request as required by the Freedom of Information Act. If the commissioner, after consultation with the chief executive officer of the applicable agency, believes the requested record is exempt from disclosure pursuant to subdivision (19) of subsection (b) of this section, the commissioner may direct the agency to withhold such record from such person. In any appeal brought under the provisions of section 1-206 of the Freedom of Information Act for denial of access to records for any of the reasons described in subdivision (19) of subsection (b) of this section, such appeal shall be against the chief executive officer of the executive branch state agency or the municipal, district or regional agency that issued the directive to withhold such record pursuant to subdivision (19) of subsection (b) of this section, exclusively, or, in the case of records concerning Judicial Department facilities, the Chief Court Administrator or, in the case of records concerning the Legislative Department, the executive director of the Joint Committee on Legislative Management.
Delaware: 29 Del. Code Ann. §10002(17a)

(17a) The following records, which, if copied or inspected, could jeopardize the security of any structure owned by the State or any of its political subdivisions, or could facilitate the planning of a terrorist attack, or could endanger the life or physical safety of an individual:

1. Response procedures or plans prepared to prevent or respond to emergency situations, the disclosure of which would reveal vulnerability assessments, specific tactics, specific emergency procedures or specific security procedures.

2. Building plans, blueprints, schematic drawings, diagrams, operational manuals or other records of mass transit facilities, bridges, tunnels, emergency response facilities or structures, buildings where hazardous materials are used or stored, arenas, stadiums, waste and water systems, electric transmission lines and substations, high-pressure natural gas pipelines and compressor stations, and telecommunications networks facilities and switching equipment, the disclosure of which would reveal the building's or structure's internal layout, specific location, life, safety and support systems, structural elements, surveillance techniques, alarm or security systems or technologies, operational and transportation plans or protocols, or personnel deployments. Records that disclose the substances being used or stored on a given piece of property are public records; however, records which disclose the specific location on that property of the substances being used or stored may be disclosed only if the chief administrative officer of the agency from which the record is requested determines that disclosure will not jeopardize the security of any structure owned by the State or any of its political subdivisions, or will not facilitate the planning of a terrorist attack, or will not endanger the life or physical safety of an individual.

3. Records of any building or structure operated by the State or any of its political subdivisions, the disclosure of which would reveal the building's or structure's life, safety and support systems, surveillance techniques, alarm or security systems or technologies, operational and evacuation plans or protocols, or personnel deployments.

4. Records prepared to prevent or respond to emergency situations identifying or describing the name, location, pharmaceutical cache, contents, capacity, equipment, physical features or capabilities of individual medical facilities, storage facilities, or laboratories established, maintained or regulated by the State or any of its political subdivisions.

5. Those portions of records assembled, prepared or maintained to prevent, mitigate or respond to criminal acts, the public disclosure of which would have a substantial likelihood of threatening public safety.

District of Columbia: D.C. Statute §2-534(a)(10)

Exemptions from disclosure.

(a) The following matters may be exempt from disclosure under the provisions of this subchapter:

(10) Any specific response plan, including any District of Columbia response plan, as that term is defined in § 7-2301(1), and any specific vulnerability assessment, either of which is intended to prevent or to mitigate an act of terrorism, as that term is defined in § 22-3152(1);
§119.071 General exemptions from inspection or copying of public records.

(3) Security and Firesafety

(a)1. As used in this paragraph, the term “security or firesafety system plan” includes all:

   a. Records, information, photographs, audio and visual presentations, schematic diagrams, surveys, recommendations, or consultations or portions thereof relating directly to the physical security or fire safety of the facility or revealing security or fire safety systems;

   b. Threat assessments conducted by any agency or any private entity;

   c. Threat response plans;

   d. Emergency evacuation plans;

   e. Sheltering arrangements; or

   f. Manuals for security or fire safety personnel, emergency equipment, or security or fire safety training.

2. A security or firesafety system plan or portion thereof for:

   a. Any property owned by or leased to the state or any of its political subdivisions; or

   b. Any privately owned or leased property held by an agency is confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution. This exemption is remedial in nature, and it is the intent of the Legislature that this exemption apply to security or firesafety system plans held by an agency before, on, or after the effective date of this paragraph. This paragraph is subject to the Open Government Sunset Review Act in accordance with s. 119.15 and shall stand repealed on October 2, 2023, unless reviewed and saved from repeal through reenactment by the Legislature.

3. Information made confidential and exempt by this paragraph may be disclosed:

   a. To the property owner or leaseholder;

   b. In furtherance of the official duties and responsibilities of the agency holding the information;

   c. To another local, state, or federal agency in furtherance of that agency’s official duties and responsibilities; or

   d. Upon a showing of good cause before a court of competent jurisdiction.

(b)1. Building plans, blueprints, schematic drawings, and diagrams, including draft, preliminary, and final formats, which depict the internal layout and structural elements of a building, arena, stadium, water treatment facility, or other structure owned or operated by an agency are exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution.

2. This exemption applies to building plans, blueprints, schematic drawings, and diagrams, including draft, preliminary, and final formats, which depict the internal layout and structural elements of a building, arena, stadium, water treatment facility, or other structure owned or operated by an agency before, on, or after the effective date of this act.
3. Information made exempt by this paragraph may be disclosed:
   a. To another governmental entity if disclosure is necessary for the receiving entity to perform its duties and responsibilities;
   b. To a licensed architect, engineer, or contractor who is performing work on or related to the building, arena, stadium, water treatment facility, or other structure owned or operated by an agency; or
   c. Upon a showing of good cause before a court of competent jurisdiction.

4. The entities or persons receiving such information shall maintain the exempt status of the information.


§ 50-18-72. When public disclosure not required

(a) Public disclosure shall not be required for records that are:

(25) (A) Records the disclosure of which would compromise security against sabotage or criminal or terrorist acts and the nondisclosure of which is necessary for the protection of life, safety, or public property, which shall be limited to the following:

(i) Security plans and vulnerability assessments for any public utility, technology infrastructure, building, facility, function, or activity in effect at the time of the request for disclosure or pertaining to a plan or assessment in effect at such time;

(ii) Any plan for protection against terrorist or other attacks that depends for its effectiveness in whole or in part upon a lack of general public knowledge of its details;

(iii) Any document relating to the existence, nature, location, or function of security devices designed to protect against terrorist or other attacks that depend for their effectiveness in whole or in part upon a lack of general public knowledge;

(iv) Any plan, blueprint, or other material which if made public could compromise security against sabotage, criminal, or terroristic acts; and

(v) Records of any government sponsored programs concerning training relative to governmental security measures which would identify persons being trained or instructors or would reveal information described in divisions (i) through (iv) of this subparagraph.

(B) In the event of litigation challenging nondisclosure pursuant to this paragraph by an agency of a document covered by this paragraph, the court may review the documents in question in camera and may condition, in writing, any disclosure upon such measures as the court may find to be necessary to protect against endangerment of life, safety, or public property.

(C) As used in division (i) of subparagraph (A) of this paragraph, the term “activity” means deployment or surveillance strategies, actions mandated by changes in the federal threat level, motorcades, contingency plans, proposed or alternative motorcade routes, executive and dignitary protection, planned responses to criminal or terrorist actions, after-action reports still in use, proposed or actual plans and responses to bioterrorism, and proposed or actual plans and responses to requesting and receiving the National Pharmacy Stockpile;
Guam: 5 GCA §10108

§ 10108. Limitation on Right of Inspection. Except as provided in § 10109 of this Chapter, nothing in this Chapter shall be construed to require disclosure of records that are any of the following:

(b) Records of complaints to, or investigations conducted by, or records of intelligence information, or security procedures or information, of an agency or its personnel.

(i) All existing privileges or confidential records or other information expressly protected under the law shall not be abrogated by this Act.

(j) Records specifically pertaining to security procedures, passwords, combinations, access codes, electronic or computer user I.D.s, policies or procedures on security.


§92F-13. Government records; exceptions to general rule. This part shall not require disclosure of:

(3) Government records that, by their nature, must be confidential in order for the government to avoid the frustration of a legitimate government function;

(4) Government records which, pursuant to state or federal law including an order of any state or federal court, are protected from disclosure.

Idaho: Idaho Code §74-105(4)(b)

74-105. Records Exempt from Disclosure -- Law Enforcement Records, Investigatory Records of Agencies, Evacuation and Emergency Response Plans, Worker’s Compensation. The following records are exempt from disclosure:

(4)(b) Records, other than public expenditure records, related to proposed or existing critical infrastructure held by or in the custody of any public agency only when the disclosure of such information is reasonably likely to jeopardize the safety of persons, property or the public safety. Such records may include emergency evacuation, escape or other emergency response plans, vulnerability assessments, operation and security manuals, plans, blueprints or security codes. For purposes of this section, “system” includes electrical, computer and telecommunication systems, electric power (including production, generating, transportation, transmission and distribution), heating, ventilation, and air conditioning. For purposes of this subsection, “critical infrastructure” means any system or asset, whether physical or virtual, so vital to the state of Idaho, including its political subdivisions, that the incapacity or destruction of such system or asset would have a debilitating impact on state or national economic security, state or national public health or safety or any combination of those matters.
Illinois: 5 ILCS 140/7(1)(k,o,v)

Sec. 7. Exemptions.

(1) When a request is made to inspect or copy a public record that contains information that is exempt from disclosure under this Section, but also contains information that is not exempt from disclosure, the public body may elect to redact the information that is exempt. The public body shall make the remaining information available for inspection and copying. Subject to this requirement, the following shall be exempt from inspection and copying:

(k) Architects’ plans, engineers’ technical submissions, and other construction related technical documents for projects not constructed or developed in whole or in part with public funds and the same for projects constructed or developed with public funds, including but not limited to power generating and distribution stations and other transmission and distribution facilities, water treatment facilities, airport facilities, sport stadiums, convention centers, and all government owned, operated, or occupied buildings, but only to the extent that disclosure would compromise security.

(o) Administrative or technical information associated with automated data processing operations, including but not limited to software, operating protocols, computer program abstracts, file layouts, source listings, object modules, load modules, user guides, documentation pertaining to all logical and physical design of computerized systems, employee manuals, and any other information that, if disclosed, would jeopardize the security of the system or its data or the security of materials exempt under this Section.

(v) Vulnerability assessments, security measures, and response policies or plans that are designed to identify, prevent, or respond to potential attacks upon a community’s population or systems, facilities, or installations, the destruction or contamination of which would constitute a clear and present danger to the health or safety of the community, but only to the extent that disclosure could reasonably be expected to jeopardize the effectiveness of the measures or the safety of the personnel who implement them or the public. Information exempt under this item may include such things as details pertaining to the mobilization or deployment of personnel or equipment, to the operation of communication systems or protocols, or to tactical operations.
Indiana: Ind. Code 5-14-3-4(4)(b)(19)

IC 5-14-3-4 Records and recordings exempted from disclosure; time limitations; destruction of records.

Sec. 4(b) Except as otherwise provided by subsection (a), the following public records shall be excepted from section 3 of this chapter at the discretion of a public agency:

(19) A record or a part of a record, the public disclosure of which would have a reasonable likelihood of threatening public safety by exposing a vulnerability to terrorist attack. A record described under this subdivision includes the following:

(A) A record assembled, prepared, or maintained to prevent, mitigate, or respond to an act of terrorism under IC 35-47-12-1 or an act of agricultural terrorism under IC 35-47-12-2.

(B) Vulnerability assessments.

(C) Risk planning documents.

(D) Needs assessments.

(E) Threat assessments.

(F) Intelligence assessments.

(G) Domestic preparedness strategies.

(H) The location of community drinking water wells and surface water intakes.

(I) The emergency contact information of emergency responders and volunteers.

(J) Infrastructure records that disclose the configuration of critical systems such as communication, electrical, ventilation, water, and wastewater systems.
Iowa: Iowa Code §22.7(45),(50),(71)

22.7 Confidential records. The following public records shall be kept confidential, unless otherwise ordered by a court, by the lawful custodian of the records, or by another person duly authorized to release such information:

45. The critical asset protection plan or any part of the plan prepared pursuant to section 29C.8 and any information held by the department of homeland security and emergency management that was supplied to the department by a public or private agency or organization and used in the development of the critical asset protection plan to include, but not be limited to, surveys, lists, maps, or photographs. Communications and asset information not required by law, rule, or procedure that are provided to the director by persons outside of government and for which the director has signed a nondisclosure agreement are exempt from public disclosures. The department of homeland security and emergency management may provide all or part of the critical asset plan to federal, state, or local governmental agencies which have emergency planning or response functions if the director is satisfied that the need to know and intended use are reasonable. An agency receiving critical asset protection plan information from the department shall not redisseminate the information without prior approval of the director.

50. Information and records concerning physical infrastructure, cyber security, critical infrastructure, security procedures, or emergency preparedness developed, maintained, or held by a government body for the protection of life or property, if disclosure could reasonably be expected to jeopardize such life or property.

   a. Such information and records include but are not limited to information directly related to vulnerability assessments; information contained in records relating to security measures such as security and response plans, security codes and combinations, passwords, restricted area passes, keys, and security or response procedures; emergency response protocols; and information contained in records that if disclosed would significantly increase the vulnerability of critical physical systems or infrastructures to attack.

   b. For purposes of this subsection, “cyber security information and records” include but are not limited to information and records relating to cyber security defenses, threats, attacks, or general attempts to attack cyber system operations.

71. Information and records related to cyber security information or critical infrastructure, the disclosure of which may expose or create vulnerability to critical infrastructure systems, held by the utilities board of the department of commerce or the department of homeland security and emergency management for purposes relating to the safeguarding of telecommunications, electric, water, sanitary sewage, storm water drainage, energy, hazardous liquid, natural gas, or other critical infrastructure systems. For purposes of this subsection, “cyber security information” includes but is not limited to information relating to cyber security defenses, threats, attacks, or general attempts to attack cyber system operations.

45-221. Certain records not required to be open; separation of open and closed information required; statistics and records over 70 years old open. (a) Except to the extent disclosure is otherwise required by law, a public agency shall not be required to disclose:

(12) Records of emergency or security information or procedures of a public agency, or plans, drawings, specifications or related information for any building or facility which is used for purposes requiring security measures in or around the building or facility or which is used for the generation or transmission of power, water, fuels or communications, if disclosure would jeopardize security of the public agency, building or facility.

(32) Engineering and architectural estimates made by or for any public agency relative to public improvements.

(45) Records, other than criminal investigation records, the disclosure of which would pose a substantial likelihood of revealing security measures that protect:

(A) Systems, facilities or equipment used in the production, transmission or distribution of energy, water or communications services;

(B) transportation and sewer or wastewater treatment systems, facilities or equipment; or

(C) private property or persons, if the records are submitted to the agency.

For purposes of this paragraph, security means measures that protect against criminal acts intended to intimidate or coerce the civilian population, influence government policy by intimidation or coercion or to affect the operation of government by disruption of public services, mass destruction, assassination or kidnapping. Security measures include, but are not limited to, intelligence information, tactical plans, resource deployment and vulnerability assessments.

(54) Records of a utility concerning information about cyber security threats, attacks or general attempts to attack utility operations provided to law enforcement agencies, the state corporation commission, the federal energy regulatory commission, the department of energy, the southwest power pool, the North American electric reliability corporation, the federal communications commission or any other federal, state or regional organization that has a responsibility for the safeguarding of telecommunications, electric, potable water, waste water disposal or treatment, motor fuel or natural gas energy supply systems.
Kentucky: *Ky. Rev. Stat. §61.878(m)*

61.878 Certain public records exempted from inspection except on order of court -- Restriction of state employees to inspect personnel files prohibited.

(1) The following public records are excluded from the application of KRS 61.870 to 61.884 and shall be subject to inspection only upon order of a court of competent jurisdiction, except that no court shall authorize the inspection by any party of any materials pertaining to civil litigation beyond that which is provided by the Rules of Civil Procedure governing pretrial discovery:

(m) 1. Public records the disclosure of which would have a reasonable likelihood of threatening the public safety by exposing a vulnerability in preventing, protecting against, mitigating, or responding to a terrorist act and limited to:

   a. Criticality lists resulting from consequence assessments;
   b. Vulnerability assessments;
   c. Antiterrorism protective measures and plans;
   d. Counterterrorism measures and plans;
   e. Security and response needs assessments;
   f. Infrastructure records that expose a vulnerability referred to in this subparagraph through the disclosure of the location, configuration, or security of critical systems, including public utility critical systems. These critical systems shall include but not be limited to information technology, communication, electrical, fire suppression, ventilation, water, wastewater, sewage, and gas systems;
   g. The following records when their disclosure will expose a vulnerability referred to in this subparagraph: detailed drawings, schematics, maps, or specifications of structural elements, floor plans, and operating,
utility, or security systems of any building or facility owned, occupied, leased, or maintained by a public agency; and

h. Records when their disclosure will expose a vulnerability referred to in this subparagraph and that describe the exact physical location of hazardous chemical, radiological, or biological materials.

2. As used in this paragraph, “terrorist act” means a criminal act intended to:

a. Intimidate or coerce a public agency or all or part of the civilian population;

b. Disrupt a system identified in subparagraph 1.f. of this paragraph; or

c. Cause massive destruction to a building or facility owned, occupied, leased, or maintained by a public agency.

3. On the same day that a public agency denies a request to inspect a public record for a reason identified in this paragraph, that public agency shall forward a copy of the written denial of the request, referred to in KRS 61.880(1), to the executive director of the Kentucky Office of Homeland Security and the Attorney General.

4. Nothing in this paragraph shall affect the obligations of a public agency with respect to disclosure and availability of public records under state environmental, health, and safety programs.

5. The exemption established in this paragraph shall not apply when a member of the Kentucky General Assembly seeks to inspect a public record identified in this paragraph under the Open Records Law;

Louisiana: La. Rev. Stat. §44:3(A)(3), §44.3.1

§44.3. Records of prosecutive, investigative, and law enforcement agencies and communications districts.

A. Nothing in this Chapter shall be construed to require disclosures of records, or the information contained therein, held by the offices of the attorney general, district attorneys, sheriffs, police departments, Department of Public Safety and Corrections, marshals, investigators, public health investigators, correctional agencies, communications districts, intelligence agencies, Council on Peace Officer Standards and Training, Louisiana Commission on Law Enforcement and Administration of Criminal Justice, or publicly owned water districts of the state, which records are:

(3) Records containing security procedures, investigative training information or aids, investigative techniques, investigative technical equipment or instructions on the use thereof, criminal intelligence information pertaining to terrorist-related activity, or threat or vulnerability assessments collected or obtained in the prevention of terrorist-related activity, including but not limited to physical security information, proprietary information, operational plans, and the analysis of such information, or internal security information; or

§44.3.1. Certain records pertaining to terrorist-related activity. Nothing in this Chapter shall be construed to require disclosure of records containing security procedures, criminal intelligence information pertaining to terrorist-related activity, or threat or vulnerability assessments created, collected, or obtained in the prevention of terrorist-related activity, including but not limited to physical security information, proprietary information, operational plans, and the analysis of such information, or internal security information.

§402. Definitions

3. Public records. The term “public records” means any written, printed or graphic matter or any mechanical or electronic data compilation from which information can be obtained, directly or after translation into a form susceptible of visual or aural comprehension, that is in the possession or custody of an agency or public official of this State or any of its political subdivisions, or is in the possession or custody of an association, the membership of which is composed exclusively of one or more of any of these entities, and has been received or prepared for use in connection with the transaction of public or governmental business or contains information relating to the transaction of public or governmental business, except:

L. Records describing security plans, security procedures or risk assessments prepared specifically for the purpose of preventing or preparing for acts of terrorism, but only to the extent that release of information contained in the record could reasonably be expected to jeopardize the physical safety of government personnel or the public. Information contained in records covered by this paragraph may be disclosed to the Legislature or, in the case of a political or administrative subdivision, to municipal officials or board members under conditions that protect the information from further disclosure. For purposes of this paragraph, “terrorism” means conduct that is designed to cause serious bodily injury or substantial risk of bodily injury to multiple persons, substantial damage to multiple structures whether occupied or unoccupied or substantial physical damage sufficient to disrupt the normal functioning of a critical infrastructure;

M. Records or information describing the architecture, design, access authentication, encryption or security of information technology infrastructure, systems and software. Records or information covered by this paragraph may be disclosed to the Legislature or, in the case of a political or administrative subdivision, to municipal officials or board members under conditions that protect the information from further disclosure;
Maryland: MD Gen Provisions Code § 4-352

§ 4-352. Information related to Emergency Management.

(a) Subject to subsections (b) and (c) of this section, a custodian may deny inspection of:

(1) response procedures or plans prepared to prevent or respond to emergency situations, the disclosure of which would reveal vulnerability assessments, specific tactics, specific emergency procedures, or specific security procedures;

(2) (i) building plans, blueprints, schematic drawings, diagrams, operational manuals, or any other records of ports and airports and any other mass transit facilities, bridges, tunnels, emergency response facilities or structures, buildings where hazardous materials are stored, arenas, stadiums, waste and water systems, and any other building, structure, or facility, the disclosure of which would reveal the building's, structure's, or facility's internal layout, specific location, life, safety, and support systems, structural elements, surveillance techniques, alarm or security systems or technologies, operational and transportation plans or protocols, or personnel deployments; or

(ii) records of any other building, structure, or facility, the disclosure of which would reveal the building's, structure's, or facility's life, safety, and support systems, surveillance techniques, alarm or security systems or technologies, operational and evacuation plans or protocols, or personnel deployments; or

(3) records that:

(i) are prepared to prevent or respond to emergency situations; and

(ii) identify or describe the name, location, pharmaceutical cache, contents, capacity, equipment, physical features, or capabilities of individual medical facilities, storage facilities, or laboratories.

(b) Circumstances under which denial is permissible. -- The custodian may deny inspection of a part of a public record under subsection (a) of this section only to the extent that the inspection would:

(1) jeopardize the security of any building, structure, or facility;

(2) facilitate the planning of a terrorist attack; or

(3) endanger the life or physical safety of an individual.

(c) Circumstances under which denial is prohibited. --

(1) This subsection does not apply to the records of any building, structure, or facility owned or operated by the State or any political subdivision.

(2) A custodian may not deny inspection of a public record under subsection (a) or (b) of this section that relates to a building, structure, or facility that has been subjected to a catastrophic event, including a fire, an explosion, or a natural disaster.

(3) Subject to subsections (a) and (b) of this section, a custodian may not deny inspection of a public record that relates to an inspection of or issuance of a citation concerning a building, structure, or facility by an agency of the State or any political subdivision.
Massachusetts: Mass. Gen. L. Ch. 4, §7.26(n)

Section 7: Definitions of statutory terms; statutory construction

26. “Public records” shall mean all books, papers, maps, photographs, recorded tapes, financial statements, statistical tabulations, or other documentary materials or data, regardless of physical form or characteristics, made or received by any officer or employee of any agency, executive office, department, board, commission, bureau, division or authority of the commonwealth, or of any political subdivision thereof, or of any authority established by the general court to serve a public purpose, or any person, corporation, association, partnership or other legal entity which receives or expends public funds for the payment or administration of pensions for any current or former employees of the commonwealth or any political subdivision as defined in section 1 of chapter 32, unless such materials or data fall within the following exemptions in that they are:

(n) records, including, but not limited to, blueprints, plans, policies, procedures and schematic drawings, which relate to internal layout and structural elements, security measures, emergency preparedness, threat or vulnerability assessments, or any other records relating to the security or safety of persons or buildings, structures, facilities, utilities, transportation, cyber security or other infrastructure located within the commonwealth, the disclosure of which, in the reasonable judgment of the record custodian, subject to review by the supervisor of public records under subsection (c) of section 10 of chapter 66, is likely to jeopardize public safety or cyber security.


15.243(1) A public body may exempt from disclosure as a public record under this act any of the following:

(y) Records or information of measures designed to protect the security or safety of persons or property, or the confidentiality, integrity, or availability of information systems, whether public or private, including, but not limited to, building, public works, and public water supply designs to the extent that those designs relate to the ongoing security measures of a public body, capabilities and plans for responding to a violation of the Michigan anti-terrorism act, chapter LXXXIII-A of the Michigan penal code, 1931 PA 328, MCL 750.543a to 750.543z, emergency response plans, risk planning documents, threat assessments, domestic preparedness strategies, and cybersecurity plans, assessments, or vulnerabilities, unless disclosure would not impair a public body’s ability to protect the security or safety of persons or property or unless the public interest in disclosure outweighs the public interest in nondisclosure in the particular instance.

13.03 Access to Government Data.

(1) Public data. All government data collected, created, received, maintained or disseminated by a government entity shall be public unless classified by statute, or temporary classification pursuant to section 13.06, or federal law, as nonpublic or protected nonpublic, or with respect to data on individuals, as private or confidential. The responsible authority in every government entity shall keep records containing government data in such an arrangement and condition as to make them easily accessible for convenient use. Photographic, photostatic, microphotographic, or microfilmed records shall be considered as accessible for convenient use regardless of the size of such records.

(3)(f) If the responsible authority or designee determines that the requested data is classified so as to deny the requesting person access, the responsible authority or designee shall inform the requesting person of the determination either orally at the time of the request, or in writing as soon after that time as possible, and shall cite the specific statutory section, temporary classification, or specific provision of federal law on which the determination is based. Upon the request of any person denied access to data, the responsible authority or designee shall certify in writing that the request has been denied and cite the specific statutory section, temporary classification, or specific provision of federal law upon which the denial was based.

13.06 Temporary Classification.

(1) Application to commissioner [means the commissioner of the Department of Administration].

(a) Notwithstanding the provisions of section 13.03, the responsible authority of a government entity may apply to the commissioner for permission to classify data or types of data on individuals as private or confidential, or data not on individuals as nonpublic or protected nonpublic, for its own use and for the use of other similar government entities on a temporary basis until a proposed statute can be acted upon by the legislature. The application for temporary classification is public.

(b) Upon receipt by the commissioner of an application for temporary classification, the data which is the subject of the application shall be deemed to be classified as set forth in the application for a period of 45 days, or until the application is disapproved, rejected, or granted by the commissioner, whichever is earlier.

(c) If the commissioner determines that an application has been submitted for purposes not consistent with this section, the commissioner may immediately reject the application, give notice of that rejection to the applicant, and return the application. When the applicant receives the notice of rejection from the commissioner, the data which was the subject of the application shall have the classification it had before the application was submitted to the commissioner.
§ 25-61-5. Public Access to Records; Denials

(1) (a) Except as otherwise provided by Sections 25-61-9 and 25-61-11, all public records are hereby declared to be public property, and any person shall have the right to inspect, copy or mechanically reproduce or obtain a reproduction of any public record of a public body in accordance with reasonable written procedures adopted by the public body concerning the cost, time, place and method of access, and public notice of the procedures shall be given by the public body, or, if a public body has not adopted written procedures, the right to inspect, copy or mechanically reproduce or obtain a reproduction of a public record of the public body shall be provided within one (1) working day after a written request for a public record is made. No public body shall adopt procedures which will authorize the public body to produce or deny production of a public record later than seven (7) working days from the date of the receipt of the request for the production of the record.

(b) If a public body is unable to produce a public record by the seventh working day after the request is made, the public body must provide a written explanation to the person making the request stating that the record requested will be produced and specifying with particularity why the records cannot be produced within the seven-day period. Unless there is mutual agreement of the parties, or the information requested is part of ongoing negotiations related to a request for competitive sealed proposals, in no event shall the date for the public body’s production of the requested records be any later than fourteen (14) working days from the receipt by the public body of the original request. Production of competitive sealed proposals in accordance with requests made pursuant to this section shall be no later than seven (7) working days after the notice of intent to award is issued to the winning proposer. Persons making a request for production of competitive sealed proposals after the notice of intent to award is issued by the public body shall have a reasonable amount of time, but in no event less than seven (7) working days after the production of the competitive sealed proposals, to protest the procurement or intended award prior to contract execution.

(2) If any public record contains material which is not exempted under this chapter, the public agency shall redact the exempted material and make the nonexempted material available for examination. Such public agency shall be entitled to charge a reasonable fee for the redaction of any exempted material, not to exceed the agency’s actual cost.

(3) Denial by a public body of a request for access to or copies of public records under this chapter shall be in writing and shall contain a statement of the specific exemption relied upon by the public body for the denial. Each public body shall maintain a file of all denials of requests for public records. Public bodies shall be required to preserve such denials on file for not less than three (3) years from the date such denials are made. This file shall be made available for inspection or copying, or both, during regular office hours to any person upon written request.

§ 25-61-11.2. Exemption for certain information technology records. The following information technology (IT) records shall be exempt from the Mississippi Public Records Act of 1983:

(a) IT infrastructure details, including network architecture, schematics, and IT system designs;
(b) Source code;
(c) Detailed hardware and software inventories;
(d) Security plans;
(e) Vulnerability reports;
(f) Security risk assessment details;
(g) Security compliance reports;
(h) Authentication credentials;
(i) Security policies and processes;
(j) Security incident reports; and
(k) Any audit, assessment, compliance report, work papers or any combination of these that if disclosed could allow unauthorized access to the state's IT assets.

Missouri: Mo. Rev. Stat §610.021(18-21)
610.021. Closed meetings and closed records authorized when, exceptions. — Except to the extent disclosure is otherwise required by law, a public governmental body is authorized to close meetings, records and votes, to the extent they relate to the following:

(18) Operational guidelines, policies and specific response plans developed, adopted, or maintained by any public agency responsible for law enforcement, public safety, first response, or public health for use in responding to or preventing any critical incident which is or appears to be terrorist in nature and which has the potential to endanger individual or public safety or health. Financial records related to the procurement of or expenditures relating to operational guidelines, policies or plans purchased with public funds shall be open. When seeking to close information pursuant to this exception, the public governmental body shall affirmatively state in writing that disclosure would impair the public governmental body’s ability to protect the security or safety of persons or real property, and shall in the same writing state that the public interest in nondisclosure outweighs the public interest in disclosure of the records;

(19) Existing or proposed security systems and structural plans of real property owned or leased by a public governmental body, and information that is voluntarily submitted by a nonpublic entity owning or operating an infrastructure to any public governmental body for use by that body to devise plans for protection of that infrastructure, the public disclosure of which would threaten public safety:

(a) Records related to the procurement of or expenditures relating to security systems purchased with public funds shall be open;

(b) When seeking to close information pursuant to this exception, the public governmental body shall affirmatively state in writing that disclosure would impair the public governmental body’s ability to protect the security or safety of persons or real property, and shall in the same writing state that the public interest in nondisclosure outweighs the public interest in disclosure of the records;

(c) Records that are voluntarily submitted by a nonpublic entity shall be reviewed by the receiving agency within ninety days of submission to
determine if retention of the document is necessary in furtherance of a state security interest. If retention is not necessary, the documents shall be returned to the nonpublic governmental body or destroyed;

(20) The portion of a record that identifies security systems or access codes or authorization codes for security systems of real property;

(21) Records that identify the configuration of components or the operation of a computer, computer system, computer network, or telecommunications network, and would allow unauthorized access to or unlawful disruption of a computer, computer system, computer network, or telecommunications network of a public governmental body. This exception shall not be used to limit or deny access to otherwise public records in a file, document, data file or database containing public records. Records related to the procurement of or expenditures relating to such computer, computer system, computer network, or telecommunications network, including the amount of moneys paid by, or on behalf of, a public governmental body for such computer, computer system, computer network, or telecommunications network shall be open;

Montana: Mont. Code Ann. §2-6-1003

2-6-1003. Access to public information -- safety and security exceptions -- Montana historical society exception.

(1) Except as provided in subsections (2) and (3), every person has a right to examine and obtain a copy of any public information of this state.

(2) A public officer may withhold from public scrutiny information relating to individual or public safety or the security of public facilities, including public schools, jails, correctional facilities, private correctional facilities, and prisons, if release of the information jeopardizes the safety of facility personnel, the public, students in a public school, or inmates of a facility. A public officer may not withhold from public scrutiny any more information than is required to protect individual or public safety or the security of public facilities.

Nebraska: Neb. Rev. Stat. §84-712.05(8)

84-712.05. Records which may be withheld from the public; enumerated. The following records, unless publicly disclosed in an open court, open administrative proceeding, or open meeting or disclosed by a public entity pursuant to its duties, may be withheld from the public by the lawful custodian of the records:

(8) Information solely pertaining to protection of the security of public property and persons on or within public property, such as specific, unique vulnerability assessments or specific, unique response plans, either of which is intended to prevent or mitigate criminal acts the public disclosure of which would create a substantial likelihood of endangering public safety or property; computer or communications network schema, passwords, and user identification names; guard schedules; lock combinations; or public utility infrastructure specifications or design drawings the public disclosure of which would create a substantial likelihood of endangering public safety or property, unless otherwise provided by state or federal law;
Nevada: NRS 239C.210, NRS 239C.250, and NRS 239C.270

NRS 239C.210 Confidentiality of certain documents, records or other items of information upon declaration of Governor; penalties; decennial review.

1. A document, record or other item of information described in subsection 2 that is prepared and maintained for the purpose of preventing or responding to an act of terrorism is confidential, not subject to subpoena or discovery, not subject to inspection by the general public and may only be inspected by or released to:

(a) Public safety and public health personnel; and

(b) Except as otherwise provided in this subsection, the Legislative Auditor conducting a postaudit pursuant to NRS 218G.010 to 218G.555, inclusive, if the Governor determines, by executive order, that the disclosure or release of the document, record or other item of information would thereby create a substantial likelihood of compromising, jeopardizing or otherwise threatening the public health, safety or welfare. Any information that is inspected by or released to the Legislative Auditor pursuant to this subsection is not subject to the exception from confidentiality set forth in NRS 218G.130. The Legislative Auditor may confirm that vulnerability assessments have been submitted to or are in the possession of a state agency that is the subject of a postaudit, but the assessments must not be inspected by or released to the Legislative Auditor. An employee of the Audit Division of the Legislative Counsel Bureau who is conducting a postaudit that includes access to documents or information subject to the provisions of this section must be properly cleared through federal criteria or state or local background investigation and instructed, trained or certified, as applicable, regarding the security sensitivity of the documents or information.

2. The types of documents, records or other items of information subject to executive order pursuant to subsection 1 are as follows:

(a) Assessments, plans or records that evaluate or reveal the susceptibility of fire stations, police stations and other law enforcement stations to acts of terrorism or other related emergencies.

(b) Drawings, maps, plans or records that reveal the critical infrastructure of primary buildings, facilities and other structures used for storing, transporting or transmitting water or electricity, natural gas or other forms of energy, fiber optic cables, microwave towers or other vertical assets used for the transmission or receipt of data or communications used by response agencies and public safety and public health personnel.

(c) Documents, records or other items of information which may reveal the details of a specific emergency response plan or other tactical operations by a response agency and any training relating to such emergency response plans or tactical operations.

(d) Handbooks, manuals or other forms of information detailing procedures to be followed by response agencies in the event of an act of terrorism or other related emergency.

(e) Documents, records or other items of information that reveal information pertaining to specialized equipment used for covert, emergency or tactical operations of a response agency, other than records relating to expenditures for such equipment.
(f) Documents, records or other items of information regarding critical telecommunications facilities and the infrastructure and security of radio frequencies for transmissions used by response agencies, including, without limitation:

(1) Access codes, passwords or programs used to ensure the security of radio frequencies for transmissions used by response agencies;

(2) Procedures and processes used to ensure the security of radio frequencies for transmissions used by response agencies; and

(3) Plans used to re-establish security and service with respect to radio frequencies for transmissions used by response agencies after security has been breached or service has been interrupted.

(g) Vulnerability assessments and emergency response plans of utilities, public entities and private businesses in this State. As used in this paragraph, “public entities” means departments, agencies or instrumentalities of the State, any of its political subdivisions or tribal governments. The term includes general improvement districts.

NRS 239C.250 Response plans of political subdivisions: Confidentiality

1. Each political subdivision shall adopt and maintain a response plan. Each new or revised plan must be filed within 10 days after adoption or revision with:
(a) The Division; and

(b) Each response agency that provides services to the political subdivision.

2. The response plan required by subsection 1 must include:

(a) A drawing or map of the layout and boundaries of the political subdivision;

(b) A drawing or description of the streets and highways within, and leading into and out of, the political subdivision, including any approved routes for evacuation;

(c) The location and inventory of emergency response equipment and resources within the political subdivision;

(d) The location of any unusually hazardous substances within the political subdivision;

(e) A telephone number that may be used by residents of the political subdivision to receive information and to make reports with respect to an act of terrorism or related emergency;

(f) The location of one or more emergency response command posts that are located within the political subdivision;

(g) A depiction of the location of each police station, sheriff’s office and fire station that is located within the political subdivision;

(h) Plans for the continuity of the operations and services of the political subdivision, which plans must be consistent with the provisions of NRS 239C.260; and

(i) Any other information that the Commission may determine to be relevant.

3. Except as otherwise provided in NRS 239.0115, a plan filed pursuant to the requirements of this section, including any revisions adopted thereto, is confidential and must be securely maintained by the entities with whom it is filed pursuant to subsection 1. An officer, employee or other person to whom the plan is entrusted by the entity with whom it is filed shall not disclose the contents of such a plan except:

(a) Upon the lawful order of a court of competent jurisdiction;

(b) As is reasonably necessary in the case of an act of terrorism or related emergency; or

(c) Pursuant to the provisions of NRS 239.0115.

NRS 239C.270 Vulnerability assessment and response plan of utility: Confidentiality; penalties.

1. Each utility shall:

(a) Conduct a vulnerability assessment in accordance with the requirements of the federal and regional agencies that regulate the utility; and

(b) Prepare and maintain an emergency response plan in accordance with the requirements of the federal and regional agencies that regulate the utility.
2. Each utility shall:
   
   (a) As soon as practicable but not later than December 31, 2003, submit its vulnerability assessment and emergency response plan to the Division; and
   
   (b) At least once each year thereafter, review its vulnerability assessment and emergency response plan and, as soon as practicable after its review is completed but not later than December 31 of each year, submit the results of its review and any additions or modifications to its emergency response plan to the Division.

3. Except as otherwise provided in NRS 239.0115, each vulnerability assessment and emergency response plan of a utility and any other information concerning a utility that is necessary to carry out the provisions of this section is confidential and must be securely maintained by each person or entity that has possession, custody or control of the information.

4. Except as otherwise provided in NRS 239C.210, a person shall not disclose such information, except:
   
   (a) Upon the lawful order of a court of competent jurisdiction;
   
   (b) As is reasonably necessary to carry out the provisions of this section or the operations of the utility, as determined by the Division;
   
   (c) As is reasonably necessary in the case of an emergency involving public health or safety, as determined by the Division; or
   
   (d) Pursuant to the provisions of NRS 239.0115.

5. If a person knowingly and unlawfully discloses such information or assists, solicits or conspires with another person to disclose such information, the person is guilty of:
   
   (a) A gross misdemeanor; or
   
   (b) A category C felony and shall be punished as provided in NRS 193.130 if the person acted with the intent to:
   
   (1) Commit, cause, aid, further or conceal, or attempt to commit, cause, aid, further or conceal, any unlawful act involving terrorism or sabotage; or
   
   (2) Assist, solicit or conspire with another person to commit, cause, aid, further or conceal any unlawful act involving terrorism or sabotage.

91-A:5 Exemptions. The records of the following bodies are exempted from the provisions of this chapter:

VI. Records pertaining to matters relating to the preparation for and the carrying out of all emergency functions, including training to carry out such functions, developed by local or state safety officials that are directly intended to thwart a deliberate act that is intended to result in widespread or severe damage to property or widespread injury or loss of life.


C.47:1A-1.1 Definitions. A government record shall not include the following information which is deemed to be confidential for the purposes of P.L.1963, c.73 (C.47:1A-1 et seq.) as amended and supplemented:

- Computer Security: Administrative or technical information regarding computer hardware, software and networks which, if disclosed, would jeopardize computer security;
- Building Security: Emergency or security information or procedures for any buildings or facility which, if disclosed, would jeopardize security of the building or facility or persons therein;
- Security Measures and Techniques: Security measures and surveillance techniques which, if disclosed, would create a risk to the safety of persons, property, electronic data or software;


Every person has a right to inspect public records of this state except:

(G) Tactical response plans or procedures prepared for or by the state or a political subdivision of the state, the publication of which could reveal specific vulnerabilities, risk assessments or tactical emergency security procedures that could be used to facilitate the planning or execution of a terrorist attack.

New York: **N.Y. PH Law Sec. 1125(8) and N.Y. Pub. Off. Law §47-6-87(2a.f.)**

N.Y. PH Law Sec. 1125(8)

8. The commissioner shall keep confidential:

a. all vulnerability analysis assessments and all information derived therefrom; and

b. all information determined by a water supplier to pose a security risk to the operation of a water supply system.

N.Y. Pub. Off. Law §47-6-87(2a and 2.f) Access to agency records.

Each agency shall, in accordance with its published rules, make available for public inspection and copying all records, except that such agency may deny access to records or portions thereof that:

(a) are specifically exempted from disclosure by state or federal statute;

(f) if disclosed could endanger the life or safety of any person;
Sensitive public security information.

(a) Public records, as defined in G.S. 132-1, shall not include information containing specific details of public security plans and arrangements or the detailed plans and drawings of public buildings and infrastructure facilities or plans, schedules, or other documents that include information regarding patterns or practices associated with executive protection and security.

(b) Public records as defined in G.S. 132-1 do not include plans to prevent or respond to terrorist activity, to the extent such records set forth vulnerability and risk assessments, potential targets, specific tactics, or specific security or emergency procedures, the disclosure of which would jeopardize the safety of governmental personnel or the general public or the security of any governmental facility, building, structure, or information storage system.

c) Information relating to the general adoption of public security plans and arrangements, and budgetary information concerning the authorization or expenditure of public funds to implement public security plans and arrangements, or for the construction, renovation, or repair of public buildings and infrastructure facilities shall be public records.

North Dakota: N.D. Cent. Code §44-04-24
Security system plan - Disaster and cybersecurity information - Exemption.

1. A security system plan kept by a public entity is exempt from the provisions of section 44-04-18 and section 6 of article XI of the Constitution of North Dakota.

2. As used in this section:

   a. “Critical infrastructure” means public buildings, systems, including telecommunications centers and computers, power generation plants, dams, bridges, and similar key resources, whether physical or virtual, so vital to the state that the incapacity or destruction of these systems would have a debilitating impact on security, state economic security, state public health or safety, or any combination of those matters.

   b. “Security system plan” includes all records, information, photographs, audio and visual presentations, schematic diagrams, surveys, recommendations, communications, or consultations or portions of any such plan relating directly to the physical or electronic security of a public facility, or any critical infrastructure, whether owned by or leased to the state or any of its political subdivisions, or any privately owned or leased critical infrastructure if the plan or a portion of the plan is in the possession of a public entity; threat assessments; vulnerability and capability assessments conducted by a public entity, or any private entity; threat response plans; and emergency evacuation plans.
Northern Mariana Islands: 1 CMC §9917, §9918

§ 9917. Public Records: Availability for Inspection; Cost of Copies. (a) Within 10 days of a request, all public records shall be available for inspection by any person during established office hours unless public inspection of such records is in violation of any Commonwealth or federal law; provided that, except where such records are open under any rule of court, the Commonwealth Attorney General or designated assistant attorney general and the responsible attorneys for federal agencies may determine which such records in their offices may be withheld from public inspection when such records pertain to the preparation of the prosecution or defense of any action or proceeding, prior to its commencement, to which the Commonwealth is a party, or when such records do not relate to a matter in violation of law and are deemed necessary for the protection of the character or reputation of any person.

§ 9918. Certain Personal and Other Records Exempt.

[NOTE: No existing exemption appears to cover the information that may be developed in compliance with AWIA §2013.]

Ohio: Ohio Rev. Code Ann 149.433

Exempting security and infrastructure records.

(A) As used in this section:

“Act of terrorism” has the same meaning as in section 2909.21 of the Revised Code.

“Express statement” means a written statement substantially similar to the following:

“This information is voluntarily submitted to a public office in expectation of protection from disclosure as provided by section 149.433 of the Revised Code.”

“Infrastructure record” means any record that discloses the configuration of critical systems including, but not limited to, communication, computer, electrical, mechanical, ventilation, water, and plumbing systems, security codes, or the infrastructure or structural configuration of a building.

“Infrastructure record” includes a risk assessment of infrastructure performed by a state or local law enforcement agency at the request of a property owner or manager.

“Infrastructure record” does not mean a simple floor plan that discloses only the spatial relationship of components of the building.

“Security record” means any of the following:

(1) Any record that contains information directly used for protecting or maintaining the security of a public office against attack, interference, or sabotage;

(2) Any record assembled, prepared, or maintained by a public office or public body to prevent, mitigate, or respond to acts of terrorism, including any of the following:

(a) Those portions of records containing specific and unique vulnerability assessments or specific and unique response plans either of which is intended to prevent or mitigate acts of terrorism, and communication codes or deployment plans of law enforcement or emergency response personnel;
(b) Specific intelligence information and specific investigative records shared by federal and international law enforcement agencies with state and local law enforcement and public safety agencies;

(c) National security records classified under federal executive order and not subject to public disclosure under federal law that are shared by federal agencies, and other records related to national security briefings to assist state and local government with domestic preparedness for acts of terrorism.

(3) An emergency management plan adopted pursuant to section 3313.536 of the Revised Code.

(B) (1) A record kept by a public office that is a security record is not a public record under section 149.43 of the Revised Code and is not subject to mandatory release or disclosure under that section.

(2) A record kept by a public office that is an infrastructure record of a public office, public school, or a chartered nonpublic school is not a public record under section 149.43 of the Revised Code and is not subject to mandatory release or disclosure under that section.

(3) A record kept by a public office that is an infrastructure record of a private entity may be exempted from release or disclosure under division (C) of this section.

(C) A record prepared by, submitted to, or kept by a public office that is an infrastructure record of a private entity, which is submitted to the public office for use by the public office, when accompanied by an express statement, is exempt from release or disclosure under section 149.43 of the Revised Code for a period of twenty-five years after its creation if it is retained by the public office for that length of time.

(D) Notwithstanding any other section of the Revised Code, disclosure by a public office, public employee, chartered nonpublic school, or chartered nonpublic school employee of a security record or infrastructure record that is necessary for construction, renovation, or remodeling work on any public building or project or chartered nonpublic school does not constitute public disclosure for purposes of waiving division (B) of this section and does not result in that record becoming a public record for purposes of section 149.43 of the Revised Code.

A. Any state environmental agency or public utility shall keep confidential vulnerability assessments of critical assets in both water and wastewater systems. State environmental agencies or public utilities may use the information for internal purposes or allow the information to be used for survey purposes only. The state environmental agencies or public utilities shall allow any public body to have access to the information for purposes specifically related to the public bodies function.

1. B. For purposes of this section:

2. “Public Utility” means any individual, firm, association, partnership, corporation or any combination thereof, municipal corporations or their lessees, trustees and receivers, owning or operating for compensation in this state equipment or facilities for:

a. producing, generating, transmitting, distributing, selling or furnishing electricity,

b. the conveyance, transmission, reception or communications over a telephone system,

c. transmitting directly or indirectly or distributing combustible hydrocarbon natural or synthetic natural gas for sale to the public, or

d. the transportation, delivery or furnishing of water for domestic purposes or for power.

Oregon: Or. Rev. Stat. §192.335(33)

The following public records are exempt from disclosure under ORS 192.311

(33) Information about review or approval of programs relating to the security of:

(a) Generation, storage or conveyance of:

(A) Electricity;

(B) Gas in liquefied or gaseous form;

(C) Hazardous substances as defined in ORS 453.005 (Definitions for ORS 453.005 to 453.135) (7)(a), (b) and (d);

(D) Petroleum products;

(E) Sewage; or

(F) Water.

(b) Telecommunication systems, including cellular, wireless or radio systems.

(c) Data transmissions by whatever means provided.
Pennsylvania: Pa. Stat. § 67.708(b)

Public Officers § 67.708. Exceptions for public records

(b) Exceptions. Except as provided in subsections (c) and (d), the following are exempt from access by a requester under this act:

(3) A record, the disclosure of which creates a reasonable likelihood of endangering the safety or the physical security of a building, public utility, resource, infrastructure, facility or information storage system, which may include:

(i) documents or data relating to computer hardware, source files, software and system networks that could jeopardize computer security by exposing a vulnerability in preventing, protecting against, mitigating or responding to a terrorist act;

(ii) lists of infrastructure, resources and significant special events, including those defined by the Federal Government in the National Infrastructure Protections, which are deemed critical due to their nature and which result from risk analysis; threat assessments; consequences assessments; antiterrorism protective measures and plans; counterterrorism measures and plans; and security and response needs assessments; and

(iii) building plans or infrastructure records that expose or create vulnerability through disclosure of the location, configuration or security of critical systems, including public utility systems, structural elements, technology, communication, electrical, fire suppression, ventilation, water, wastewater, sewage and gas systems.

(4) A record regarding computer hardware, software and networks, including administrative or technical records, which, if disclosed, would be reasonably likely to jeopardize computer security.

Puerto Rico: 32 L.P.R.A. § 1781

Right to inspect and copy public documents. Every citizen has a right to inspect and take a copy of any public document of Puerto Rico, except as otherwise expressly provided by law.


Definitions.

(4) “Public record” or “public records” shall mean all documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, magnetic or other tapes, electronic data processing records, computer stored data (including electronic mail messages, except specifically for any electronic mail messages of or to elected officials with or relating to those they represent and correspondence of or to elected officials in their official capacities), or other material regardless of physical form or characteristics made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency. For the purposes of this chapter, the following records shall not be deemed public:

(S) Records, reports, opinions, information, and statements required to be kept confidential by federal law or regulation or state law or rule of court.
South Carolina: S.C. Code Ann. 30-4
Section 30-4-20. Definitions.

(c) “Public record” includes all books, papers, maps, photographs, cards, tapes, recordings, or other documentary materials regardless of physical form or characteristics prepared, owned, used, in the possession of, or retained by a public body....Information relating to security plans and devices proposed, adopted, installed, or utilized by a public body, other than amounts expended for adoption, implementation, or installation of these plans and devices, is required to be closed to the public and is not considered to be made open to the public under the provisions of this act.

Section 30-4-40. Matters exempt from disclosure.

(a) A public body may but is not required to exempt from disclosure the following information:

(4) Matters specifically exempted from disclosure by statute or law.

South Dakota: S.D. Codified Law Ann 1-27-1.5
Certain records not open to inspection and copying:

(8) Information pertaining to the protection of public or private property and any person on or within public or private property including:

(a) Any vulnerability assessment or response plan intended to prevent or mitigate criminal acts;

(b) Emergency management or response;

(c) Public safety information that would create a substantial likelihood of endangering public safety or property, if disclosed;

(d) Computer or communications network schema, passwords, or user identification names;

(e) Guard schedules;

(f) Lock combinations; and

(g) Any blueprint, building plan, or infrastructure record regarding any building or facility that would expose or create vulnerability through disclosure of the location, configuration, or security of critical systems of the building or facility;

Tennessee: Tenn. Code Ann §10-7-504(a)(21) and Tenn. Code Ann §10-7-504(m)
Tenn. Code Ann §10-7-504(a)(21)

(21)(A) The following records shall be treated as confidential and shall not be open for public inspection:

(i) Records that would allow a person to identify areas of structural or operational vulnerability of a utility service provider or that would permit unlawful disruption to, or interference with, the services provided by a utility service provider;

(ii) All contingency plans of a governmental entity prepared to respond to or prevent any violent incident, bomb threat, ongoing act of violence at a school or business, ongoing act of violence at a place of public gathering, threat involving a weapon of mass destruction, or terrorist incident.
(B) Documents concerning the cost of governmental utility property, the cost of protecting governmental utility property, the cost of identifying areas of structural or operational vulnerability of a governmental utility, the cost of developing contingency plans for a governmental entity, and the identity of vendors providing goods or services to a governmental entity in connection with the foregoing shall not be confidential. However, any documents relating to these subjects shall not be made available to the public unless information that is confidential under this subsection (a) or any other provision of this chapter has been redacted or deleted from the documents.

(C) As used in this subdivision (a)(21):

(i) “Governmental entity” means the state of Tennessee or any county, municipality, city or other political subdivision of the state of Tennessee;

(ii) “Governmental utility” means a utility service provider that is also a governmental entity; and

(iii) “Utility service provider” means any entity, whether public or private, that provides electric, gas, water, sewer or telephone service, or any combination of the foregoing, to citizens of the state of Tennessee, whether or not regulated by the Tennessee public utility commission.

Tenn. Code Ann §10-7-504(m)

(m) (1) Information and records that are directly related to the security of any government building shall be maintained as confidential and shall not be open to public inspection. For purposes of this subsection (m), “government building” means any building that is owned, leased or controlled, in whole or in part, by the state of Tennessee or any county, municipality, city or other political subdivision of the state of Tennessee. Such information and records include, but are not limited to:

(A) Information and records about alarm and security systems used at the government building, including codes, passwords, wiring diagrams, plans and security procedures and protocols related to the security systems;

(B) Security plans, including security-related contingency planning and emergency response plans;

(C) Assessments of security vulnerability;

(D) Information and records that would identify those areas of structural or operational vulnerability that would permit unlawful disruption to, or interference with, the services provided by a governmental entity; and

(E) Surveillance recordings, whether recorded to audio or visual format, or both, except segments of the recordings may be made public when they include an act or incident involving public safety or security or possible criminal activity. In addition, if the recordings are relevant to a civil action or criminal prosecution, then the recordings may be released in compliance with a subpoena or an order of a court of record in accordance with the Tennessee rules of civil or criminal procedure. The court or administrative judge having jurisdiction over the proceedings shall issue appropriate protective orders, when necessary, to ensure that the information is disclosed only to appropriate persons. Release of any segment or segments of the recordings shall not be construed as waiving the confidentiality of the remaining segments of the audio or visual tape.
(2) Information made confidential by this subsection (m) shall be redacted wherever possible and nothing in this subsection (m) shall be used to limit or deny access to otherwise public information because a file or document contains confidential information.

Texas: Tex Code Ann. Sec. 552.139

Sec. 552.139. Exception: Confidentiality of Government Information Related to Security or Infrastructure Issues For Computers.

(a) Information is excepted from the requirements of Section 552.021 if it is information that relates to computer network security, to restricted information under Section 2059.055, or to the design, operation, or defense of a computer network.

(b) The following information is confidential:

(1) a computer network vulnerability report;

(2) any other assessment of the extent to which data processing operations, a computer, a computer program, network, system, or system interface, or software of a governmental body or of a contractor of a governmental body is vulnerable to unauthorized access or harm, including an assessment of the extent to which the governmental body’s or contractor’s electronically stored information containing sensitive or critical information is vulnerable to alteration, damage, erasure, or inappropriate use;

(3) a photocopy or other copy of an identification badge issued to an official or employee of a governmental body; and

(4) information directly arising from a governmental body’s routine efforts to prevent, detect, investigate, or mitigate a computer security incident, including information contained in or derived from an information security log.

(b-1) Subsection (b)(4) does not affect the notification requirements related to a breach of system security as defined by Section 521.053, Business & Commerce Code.

(c) Notwithstanding the confidential nature of the information described in this section, the information may be disclosed to a bidder if the governmental body determines that providing the information is necessary for the bidder to provide an accurate bid. A disclosure under this subsection is not a voluntary disclosure for purposes of Section 552.007.

(d) A state agency shall redact from a contract posted on the agency’s Internet website under Section 2261.253 information that is made confidential by, or excepted from required public disclosure under, this section. The redaction of information under this subsection does not exempt the information from the requirements of Section 552.021 or 552.221.

US Virgin Islands: 3 VIC §881(g)(14)

§ 881. Examination of public records

(g) Confidential records. The following public records shall be kept confidential, unless otherwise ordered by a court, by the lawful custodian of the records, or by another person duly authorized to release information:

Utah: **Utah Code Ann. §63G-2-106**

Records of security measures. The records of a governmental entity or political subdivision regarding security measures designed for the protection of persons or property, public or private, are not subject to this chapter. These records include:

1. security plans;
2. security codes and combinations, and passwords;
3. passes and keys;
4. security procedures; and
5. building and public works designs, to the extent that the records or information relate to the ongoing security measures of a public entity.


(c) The following public records are exempt from public inspection and copying:

32. With respect to publicly owned, managed, or leased structures, and only to the extent that release of information contained in the record would present a substantial likelihood of jeopardizing the safety of persons or the security of public property, final building plans, and as-built plans, including drafts of security systems within a facility, that depict the internal layout and structural elements of buildings, facilities, infrastructures, systems, or other structures owned, operated, or leased by an agency before, on, or after the effective date of this provision; emergency evacuation, escape, or other emergency response plans that have not been published for public use; and vulnerability assessments, operation and security manuals, plans, and security codes. For purposes of this subdivision, "system" shall include electrical, heating, ventilation, air conditioning, telecommunication, elevator, and security systems.

Information made exempt by this subdivision may be disclosed to another governmental entity if disclosure is necessary for the receiving entity to perform its duties and responsibilities; to a licensed architect, engineer, or contractor who is bidding on or performing work on or related to buildings, facilities, infrastructures, systems, or other structures owned, operated, or leased by the State.
Virginia: Va. Code §2.2-3705.2(14)

§ 2.2-3705.2. Exclusions to application of chapter; records relating to public safety.

The following information contained in a public record is excluded from the mandatory disclosure provisions of this chapter but may be disclosed by the custodian in his discretion, except where such disclosure is prohibited by law. Redaction of information excluded under this section from a public record shall be conducted in accordance with § 2.2-3704.01.

14. Information contained in (i) engineering, architectural, or construction drawings; (ii) operational, procedural, tactical planning, or training manuals; (iii) staff meeting minutes; or (iv) other records that reveal any of the following, the disclosure of which would jeopardize the safety or security of any person; governmental facility, building, or structure or persons using such facility, building, or structure; or public or private commercial office, multifamily residential, or retail building or its occupants:

a. Critical infrastructure information or the location or operation of security equipment and systems of any public building, structure, or information storage facility, including ventilation systems, fire protection equipment, mandatory building emergency equipment or systems, elevators, electrical systems, telecommunications equipment and systems, or utility equipment and systems;

b. Vulnerability assessments, information not lawfully available to the public regarding specific cybersecurity threats or vulnerabilities, or security plans and measures of an entity, facility, building structure, information technology system, or software program;

c. Surveillance techniques, personnel deployments, alarm or security systems or technologies, or operational or transportation plans or protocols; or

d. Interconnectivity, network monitoring, network operation centers, master sites, or systems related to the Statewide Agencies Radio System (STARS) or any other similar local or regional public safety communications system.
Washington: Wash. Rev. Code §42.56.420

Security. The following information relating to security is exempt from disclosure under this chapter:

(1) Those portions of records assembled, prepared, or maintained to prevent, mitigate, or respond to criminal terrorist acts, which are acts that significantly disrupt the conduct of government or of the general civilian population of the state or the United States and that manifest an extreme indifference to human life, the public disclosure of which would have a substantial likelihood of threatening public safety, consisting of:

(a) Specific and unique vulnerability assessments or specific and unique response or deployment plans, including compiled underlying data collected in preparation of or essential to the assessments, or to the response or deployment plans; and

(b) Records not subject to public disclosure under federal law that are shared by federal or international agencies, and information prepared from national security briefings provided to state or local government officials related to domestic preparedness for acts of terrorism;

(4) Information regarding the public and private infrastructure and security of computer and telecommunications networks, consisting of security passwords, security access codes and programs, access codes for secure software applications, security and service recovery plans, security risk assessments, and security test results to the extent that they identify specific system vulnerabilities, and other such information the release of which may increase risk to the confidentiality, integrity, or availability of security, information technology infrastructure, or assets;

West Virginia: W.Va. Code Sec. §29B-1-4

§29B-1-4. Exemptions. (a) There is a presumption of public accessibility to all public records, subject only to the following categories of information which are specifically exempt from disclosure under this article:

(9) Records assembled, prepared, or maintained to prevent, mitigate, or respond to terrorist acts or the threat of terrorist acts, the public disclosure of which threaten the public safety or the public health;

(13) Computing, telecommunications, and network security records, passwords, security codes, or programs used to respond to or plan against acts of terrorism which may be the subject of a terrorist act;

(14) Security or disaster recovery plans, risk assessments, tests, or the results of those tests;

(15) Architectural or infrastructure designs, maps, or other records that show the location or layout of the facilities where computing, telecommunications, or network infrastructure used to plan against or respond to terrorism are located or planned to be located;

(16) Codes for facility security systems; or codes for secure applications for facilities referred to in subdivision (15) of this subsection;

(17) Specific engineering plans and descriptions of existing public utility plants and equipment;
Wisconsin: Wis. Stat. §19-35(1)(a)

19.35 Access to records; fees.

(1) Right to inspection.

(a) Except as otherwise provided by law, any requester has a right to inspect any record. Substantive common law principles construing the right to inspect, copy or receive copies of records shall remain in effect. The exemptions to the requirement of a governmental body to meet in open session under s. 19.85 are indicative of public policy, but may be used as grounds for denying public access to a record only if the authority or legal custodian under s. 19.33 makes a specific demonstration that there is a need to restrict public access at the time that the request to inspect or copy the record is made.

Wyoming: Wyo. Stat. §16-4-203(b)(vi)

(a) The custodian may deny the right of inspection of the following records, unless otherwise provided by law, on the ground that disclosure to the applicant would be contrary to the public interest:

(vi) To the extent that the inspection would jeopardize the security of any structure owned, leased or operated by the state or any of its political subdivisions, facilitate the planning of a terrorist attack or endanger the life or physical safety of an individual, including:

(A) Vulnerability assessments, specific tactics, emergency procedures or security procedures contained in plans or procedures designed to prevent or respond to terrorist attacks or other security threats;

(B) Building plans, blueprints, schematic drawings, diagrams, operational manuals or other records that reveal the building’s or structure’s internal layout, specific location, life and safety and support systems, structural elements, surveillance techniques, alarms, security systems or technologies, operational and transportation plans or protocols, personnel deployments for airports and other mass transit facilities, bridges, tunnels, emergency response facilities or structures, buildings where hazardous materials are stored, arenas, stadiums and waste and water systems;

(C) Records of any other building or structure owned, leased or operated by the state or any of its political subdivisions that reveal the building’s or structure’s life and safety systems, surveillance techniques, alarm or security systems or technologies, operational and evacuation plans or protocols or personnel deployments; and

(D) Records prepared to prevent or respond to terrorist attacks or other security threats identifying or describing the name, location, pharmaceutical cache, contents, capacity, equipment, physical features, or capabilities of individual medical facilities, storage facilities or laboratories established, maintained, or regulated by the state or any of its political subdivisions.