**5432-S.E AMH WALJ H1497.1 - NOT FOR FLOOR USE**

**ESSB 5432** - H AMD TO SGOV COMM AMD (H-1275.1/21) **549**

By Representative Walsh

**NOT ADOPTED 04/06/2021**

On page 1, after line 2, strike all material through "repealed." on page 8, line 29 and insert the following:

"NEW SECTION. **Sec.**  A new section is added to chapter 43.105 RCW to read as follows:

(1) The office of cybersecurity and information oversight is created as an agency of state government.

(2)(a) The governor with the consent of the senate shall appoint a state chief information security officer, who is the director of the office of cybersecurity. The state chief information security officer shall receive a salary as determined by the governor. If a vacancy occurs in the position while the senate is not in session, the governor shall make a temporary appointment until the next meeting of the senate at which time the governor shall present to that body his or her nomination for the position.

(b) The state chief information security officer may create such administrative structures as he or she deems appropriate and may delegate any power or duty vested in him or her by this chapter or other law.

(c) The state chief information security officer may:

(i) Appoint a confidential secretary and such deputy and assistant directors as needed to administer the agency; and

(ii) Appoint such professional, technical, and clerical assistants and employees as may be necessary to perform the duties imposed by this chapter in accordance with chapter 41.06 RCW, except as otherwise provided by law.

(3) The primary duties of the office of cybersecurity are to:

(a) Act as a central manager of the state information technology infrastructure and programs, and oversee the functions of the office of cybersecurity and the offices established within the office of cybersecurity;

(b) Establish security standards and policies to:

(i) Protect the state's information technology systems and infrastructure;

(ii) Provide appropriate governance and application of the standards and policies across information technology resources used by the state; and

(iii) Ensure the confidentiality, availability, and integrity of the information transacted, stored, or processed in the state's information technology systems and infrastructure;

(c) Develop a centralized cybersecurity protocol for protecting and managing state information technology assets and infrastructure;

(d) Detect and respond to security incidents consistent with information security standards and policies;

(e) Create a model incident response plan for state agency adoption, with the office of cybersecurity as the incident response coordinator for incidents that:

(i) Impact multiple agencies;

(ii) Impact more than 10,000 citizens;

(iii) Involve a nation state actor; or

(iv) Are likely to be in the public domain;

(f) Ensure the continuity of state business and information resources that support the operations and assets of state agencies in the event of a security incident;

(g) Provide formal guidance to state agencies on leading practices and applicable standards to ensure a whole government approach to cybersecurity, which shall include, but not be limited to, guidance regarding:

(i) The configuration and architecture of agencies' information technology systems, infrastructure, and assets;

(ii) Governance, compliance, and oversight; and

(iii) Incident investigation and response;

(h) Serve as a resource for local and municipal governments in Washington in the area of cybersecurity;

(i) Develop a service catalog of cybersecurity services to be offered to state and local governments;

(j) Collaborate with state agencies in developing standards, functions, and services in order to ensure state agency regulatory environments are understood and considered as part of an enterprise cybersecurity response;

(k) Define core services that must be managed by state agency information technology security programs; and

(l) Perform all other matters and things necessary to carry out the purposes of this chapter.

(4) The office of cybersecurity is also established with broad flexibility to adapt its operations and service catalog to address the needs of customer agencies, and to do so in the most cost-effective ways.

(5) In performing its duties, the office of cybersecurity must address the highest levels of security required to protect confidential information transacted, stored, or processed in the state's information technology systems and infrastructure that is specifically protected from disclosure by state or federal law and for which strict handling requirements are mandatory.

(6) In executing its duties under subsection (3) of this section, the office of cybersecurity shall use or rely upon existing, industry standard, widely adopted cybersecurity standards, with a preference for United States federal standards.

(7) Each state agency, institution of higher education, the legislature, and the judiciary must develop an information technology security program consistent with the office of cybersecurity's standards and policies.

(8)(a) Each state agency information technology security program must adhere to the office of cybersecurity's security standards and policies. Each state agency must review and update its program annually, certify to the office of cybersecurity that its program is in compliance with the office of cybersecurity's security standards and policies, and provide the office of cybersecurity with a list of the agency's cybersecurity business needs and agency program metrics.

(b) The office of cybersecurity shall require each state agency to obtain an independent compliance audit of its information technology security program and controls at least once every three years to determine whether the state agency's information technology security program is in compliance with the standards and policies established by the agency and that security controls identified by the state agency in its security program are operating efficiently.

(c) If a review or an audit conducted under (a) or (b) of this subsection identifies any failure to comply with the standards and policies of the office of cybersecurity or any other material cybersecurity risk, the office of cybersecurity must require the state agency to formulate and implement a plan to resolve the failure or risk. On an annual basis, the office of cybersecurity must provide a confidential report to the governor and appropriate committees of the legislature identifying and describing the cybersecurity risk or failure to comply with the office of cybersecurity's security standards and policies, as well as the agency's plan to resolve such failure or risk. Risks that are not mitigated are to be tracked by the office of cybersecurity and reviewed with the governor and the chair and ranking member of the appropriate committees of the legislature on a quarterly basis.

(d) The reports produced, and information compiled, pursuant to this subsection (8) are confidential and may not be disclosed under chapter 42.56 RCW.

(9) In the case of institutions of higher education, the judiciary, and the legislature, each information technology security program must be comparable to the intended outcomes of the office of cybersecurity's security standards and policies.

(10) By January 15th of each year, and in compliance with RCW 43.01.036, the office of cybersecurity must submit a report to the appropriate committees of the legislature that details the efficacy and cost-effectiveness of the state's efforts to protect the state's information technology systems and infrastructure from cybersecurity threats and attacks.

NEW SECTION. **Sec.**  A new section is added to chapter 43.105 RCW to read as follows:

(1) By July 1, 2022, the office of cybersecurity, in collaboration with state agencies, shall develop a catalog of cybersecurity services and functions for the office of cybersecurity to perform and, in compliance with RCW 43.01.036, submit a report to the legislature and governor. The report must include, but is not limited to:

(a) Cybersecurity services and functions to include in the office of cybersecurity's catalog of services that should be performed by the office of cybersecurity;

(b) Core capabilities and competencies of the office of cybersecurity;

(c) Security functions which should remain within state agency information technology security programs;

(d) A recommended model for accountability of state agency security programs to the office of cybersecurity; and

(e) The cybersecurity services and functions required to protect confidential information transacted, stored, or processed in the state's information technology systems and infrastructure that is specifically protected from disclosure by state or federal law and for which strict handling requirements are mandatory.

(2) The office of cybersecurity shall update and publish its catalog of services and performance metrics on a biennial basis. The office of cybersecurity shall use data and information provided from agency security programs to inform the updates to its catalog of services and performance metrics.

(3) To ensure alignment with enterprise information technology security strategy, the office of cybersecurity shall develop a process for reviewing and evaluating agency proposals for additional cybersecurity services consistent with RCW 43.105.255.

(4) The office of cybersecurity shall establish rates and fees for services provided in the catalog of services published pursuant to this section.

NEW SECTION. **Sec.**  A new section is added to chapter 43.105 RCW to read as follows:

(1) In the event of a major cybersecurity incident, as defined in policy established by the office of cybersecurity in accordance with section 1 of this act, state agencies must report that incident to the office of cybersecurity within 24 hours of discovering the incident.

(2) State agencies must provide the office of cybersecurity with contact information for any external parties who may have material information related to the cybersecurity incident.

(3) Once a cybersecurity incident is reported to the office of cybersecurity, the office of cybersecurity must investigate the incident to determine the degree of severity and facilitate any necessary incident response measures to protect the enterprise.

(4) The chief information security officer or the chief information security officer's designee shall serve as the state's point of contact for all major cybersecurity incidents.

(5) The office of cybersecurity must develop a policy to implement this section.

NEW SECTION. **Sec.**  (1) The office of cybersecurity, in collaboration with the office of privacy and data protection and the office of the attorney general, shall research and examine existing best practices for data governance, data protection, the sharing of data relating to cybersecurity, and the protection of state and local governments' information technology systems and infrastructure including, but not limited to, model terms for data-sharing contracts and adherence to privacy principles.

(2) The office of cybersecurity must submit a report of its findings and identify specific recommendations to the governor and the appropriate committees of the legislature by December 1, 2021.

(3) This section expires December 31, 2021.

NEW SECTION. **Sec.**  A new section is added to chapter 39.26 RCW to read as follows:

(1) Before a state agency shares with a contractor category 3 or higher data, as defined in policy established in accordance with RCW 43.105.054, a written data-sharing agreement must be in place. Such agreements shall conform to the policies for data sharing specified by the office of cybersecurity under the authority of RCW 43.105.054.

(2) Nothing in this section shall be construed as limiting audit authorities under chapter 43.09 RCW.

NEW SECTION. **Sec.**  A new section is added to chapter 39.34 RCW to read as follows:

(1) If a public agency is requesting from another public agency category 3 or higher data, as defined in policy established in accordance with RCW 43.105.054, the requesting agency shall provide for a written agreement between the agencies that conforms to the policies of the office of cybersecurity.

(2) Nothing in this section shall be construed as limiting audit authorities under chapter 43.09 RCW.

NEW SECTION. **Sec.**  (1) The office of cybersecurity shall contract for an independent security assessment of the state agency information technology security program audits, required under section 1 of this act, that have been conducted since July 1, 2015. The independent assessment must be conducted in accordance with subsection (2) of this section. To the greatest extent practicable, the office of cybersecurity must contract for the independent security assessment using a department of enterprise services master contract or the competitive solicitation process described under chapter 39.26 RCW. If the office of cybersecurity conducts a competitive solicitation, the office of cybersecurity shall work with the department of enterprise services, office of minority and women's business enterprises, and department of veterans affairs to engage in outreach to Washington small businesses, as defined in RCW 39.26.010, and certified veteran-owned businesses, as described in RCW 43.60A.190, and encourage these entities to submit a bid.

(2) The assessment must, at a minimum:

(a) Review the state agency information technology security program audits, required under section 1 of this act, performed since July 1, 2015;

(b) Assess the content of any audit findings and evaluate the findings relative to industry standards at the time of the audit;

(c) Evaluate the state's performance in taking action upon audit findings and implementing recommendations from the audit;

(d) Evaluate the policies and standards established by the office of cybersecurity pursuant to section 1 of this act and provide recommendations for ways to improve the policies and standards; and

(e) Include recommendations, based on best practices, for both short-term and long-term programs and strategies designed to implement audit findings.

(3) A report detailing the elements of the assessment described under subsection (2) of this section must be submitted to the governor and appropriate committees of the legislature by August 31, 2022, in compliance with RCW 43.01.036. The report is confidential and may not be disclosed under chapter 42.56 RCW.

NEW SECTION. **Sec.**  A new section is added to chapter 42.56 RCW to read as follows:

The reports and information compiled pursuant to sections 1 and 7 of this act are confidential and may not be disclosed under this chapter.

**Sec.**  RCW 43.105.007 and 2015 3rd sp.s. c 1 s 101 are each amended to read as follows:

Information technology is a tool used by state agencies to improve their ability to deliver public services efficiently and effectively. Advances in information technology, including advances in hardware, software, and business processes for implementing and managing these resources, offer new opportunities to improve the level of support provided to citizens and state agencies and to reduce the per-transaction cost of these services. These advances are one component in the process of reengineering how government delivers services to citizens.

To fully realize the service improvements and cost efficiency from the effective application of information technology to its business processes, state government must establish decision-making structures that connect business processes and information technology in an operating model. Many of these business practices transcend individual agency processes and should be worked at the enterprise level. To do this requires an effective partnership of executive management, business processes owners, and providers of support functions necessary to efficiently and effectively deliver services to citizens.

To maximize the potential for information technology to contribute to government business process reengineering, the state must establish clear central authority to plan, set enterprise policies and standards, and provide project oversight and management analysis of the various aspects of a business process.

Establishing a state chief information officer as the director of the consolidated technology services agency will provide state government with the cohesive structure necessary to develop improved operating models with agency directors and reengineer business process to enhance service delivery while capturing savings.

To achieve maximum benefit from advances in information technology, the state establishes a centralized provider and procurer of certain information technology services as an ((~~agency~~)) office within the office of cybersecurity, but is hereinafter referred to as "agency," to support the needs of public agencies. This agency shall be known as the consolidated technology services agency. To ensure maximum benefit to the state, state agencies shall rely on the consolidated technology services agency for those services with a business case of broad use, uniformity, scalability, and price sensitivity to aggregation and volume.

To successfully meet public agency needs and meet its obligation as the primary service provider for these services, the ((~~consolidated technology services~~)) agency must offer high quality services at the best value. It must be able to attract an adaptable and competitive workforce, be authorized to procure services where the business case justifies it, and be accountable to its customers for the efficient and effective delivery of critical business services.

The consolidated technology services agency is established with clear accountability to the agencies it serves and to the public. This accountability will come through enhanced transparency in the agency's operation and performance. ((~~The agency is also established with broad flexibility to adapt its operations and service catalog to address the needs of customer agencies, and to do so in the most cost-effective ways.~~))

**Sec.**  RCW 43.105.020 and 2017 c 92 s 2 are each amended to read as follows:

The definitions in this section apply throughout this chapter unless the context clearly requires otherwise.

(1) "Agency" means the consolidated technology services agency, an office within the office of cybersecurity.

(2) "Board" means the technology services board.

(3) "Customer agencies" means all entities that purchase or use information technology resources, telecommunications, or services from the consolidated technology services agency.

(4) "Director" means the state chief information officer, who is the director of the consolidated technology services agency.

(5) "Enterprise architecture" means an ongoing activity for translating business vision and strategy into effective enterprise change. It is a continuous activity. Enterprise architecture creates, communicates, and improves the key principles and models that describe the enterprise's future state and enable its evolution.

(6) "Equipment" means the machines, devices, and transmission facilities used in information processing, including but not limited to computers, terminals, telephones, wireless communications system facilities, cables, and any physical facility necessary for the operation of such equipment.

(7) "Information" includes, but is not limited to, data, text, voice, and video.

(8) "Information security" means the protection of communication and information resources from unauthorized access, use, disclosure, disruption, modification, or destruction in order to:

(a) Prevent improper information modification or destruction;

(b) Preserve authorized restrictions on information access and disclosure;

(c) Ensure timely and reliable access to and use of information; and

(d) Maintain the confidentiality, integrity, and availability of information.

(9) "Information technology" includes, but is not limited to, all electronic technology systems and services, automated information handling, system design and analysis, conversion of data, computer programming, information storage and retrieval, telecommunications, requisite system controls, simulation, electronic commerce, radio technologies, and all related interactions between people and machines.

(10) "Information technology portfolio" or "portfolio" means a strategic management process documenting relationships between agency missions and information technology and telecommunications investments.

(11) "K‑20 network" means the network established in RCW 43.41.391.

(12) "Local governments" includes all municipal and quasi-municipal corporations and political subdivisions, and all agencies of such corporations and subdivisions authorized to contract separately.

(13) "Office" means the office of the state chief information officer within the consolidated technology services agency.

(14) "Office of cybersecurity" means the office of cybersecurity and information oversight.

(15) "Oversight" means a process of comprehensive risk analysis and management designed to ensure optimum use of information technology resources and telecommunications.

((~~(15)~~)) (16) "Proprietary software" means that software offered for sale or license.

((~~(16)~~)) (17) "Public agency" means any agency of this state or another state; any political subdivision or unit of local government of this state or another state including, but not limited to, municipal corporations, quasi-municipal corporations, special purpose districts, and local service districts; any public benefit nonprofit corporation; any agency of the United States; and any Indian tribe recognized as such by the federal government.

((~~(17)~~)) (18) "Public benefit nonprofit corporation" means a public benefit nonprofit corporation as defined in RCW 24.03.005 that is receiving local, state, or federal funds either directly or through a public agency other than an Indian tribe or political subdivision of another state.

((~~(18)~~)) (19) "Public record" has the definitions in RCW 42.56.010 and chapter 40.14 RCW and includes legislative records and court records that are available for public inspection.

((~~(19)~~)) (20) "Public safety" refers to any entity or services that ensure the welfare and protection of the public.

((~~(20)~~)) (21) "Security incident" means an accidental or deliberative event that results in or constitutes an imminent threat of the unauthorized access, loss, disclosure, modification, disruption, or destruction of communication and information resources.

((~~(21)~~)) (22) "State agency" means every state office, department, division, bureau, board, commission, or other state agency, including offices headed by a statewide elected official.

((~~(22)~~)) (23) "Telecommunications" includes, but is not limited to, wireless or wired systems for transport of voice, video, and data communications, network systems, requisite facilities, equipment, system controls, simulation, electronic commerce, and all related interactions between people and machines.

((~~(23)~~)) (24) "Utility-based infrastructure services" includes personal computer and portable device support, servers and server administration, security administration, network administration, telephony, email, and other information technology services commonly used by state agencies.

**Sec.**  RCW 43.105.025 and 2015 3rd sp.s. c 1 s 103 are each amended to read as follows:

(1) There is created the consolidated technology services agency, an ((~~agency of state government~~)) office within the office of cybersecurity. The agency shall be headed by a director, who is the state chief information officer. The director shall be appointed by the ((~~governor with the consent of the senate. The director shall serve at the governor's pleasure and shall receive such salary as determined by the governor. If a vacancy occurs in the position while the senate is not in session, the governor shall make a temporary appointment until the next meeting of the senate at which time he or she shall present to that body his or her nomination for the position~~)) state chief information security officer.

(2) ((~~The director shall:~~

~~(a) Appoint a confidential secretary and such deputy and assistant directors as needed to administer the agency; and~~

~~(b) Appoint such professional, technical, and clerical assistants and employees as may be necessary to perform the duties imposed by this chapter in accordance with chapter 41.06 RCW, except as otherwise provided by law.~~

~~(3) The director may create such administrative structures as he or she deems appropriate and may delegate any power or duty vested in him or her by this chapter or other law.~~

~~(4)~~)) The director shall exercise all the powers and perform all the duties prescribed by law with respect to the administration of this chapter including:

(a) Reporting to the governor and state chief information security officer any matters relating to abuses and evasions of this chapter;

(b) Accepting and expending gifts and grants that are related to the purposes of this chapter, subject to approval of the state chief information security officer;

(c) Applying for grants from public and private entities, and receiving and administering any grant funding received for the purpose and intent of this chapter, subject to approval of the state chief information security officer; and

(d) Performing other duties as are necessary and consistent with law.

**Sec.**  RCW 43.105.052 and 2015 3rd sp.s. c 1 s 104 are each amended to read as follows:

The agency shall:

(1) Make available information services to public agencies and public benefit nonprofit corporations;

(2) Establish rates and fees for services provided by the agency, except as provided under section 2 of this act;

(3) Develop a billing rate plan for a two-year period to coincide with the budgeting process. The rate plan must be subject to review at least annually by the office of financial management. The rate plan must show the proposed rates by each cost center and show the components of the rate structure as mutually determined by the agency and the office of financial management. The rate plan and any adjustments to rates must be approved by the office of financial management;

(4) Develop a detailed business plan for any service or activity to be contracted under RCW 41.06.142((~~(7)(b)~~)) (11);

(5) Develop plans for the agency's achievement of statewide goals and objectives set forth in the state strategic information technology plan required under RCW 43.105.220;

(6) Enable the standardization and consolidation of information technology infrastructure across all state agencies to support enterprise-based system development and improve and maintain service delivery; and

(7) Perform all other matters and things necessary to carry out the purposes and provisions of this chapter.

**Sec.**  RCW 43.105.054 and 2016 c 237 s 3 are each amended to read as follows:

(1) The ((~~director~~)) state chief information security officer shall establish standards and policies to govern information technology in the state of Washington.

(2) The office shall have the following powers and duties related to information services:

(a) To develop statewide standards and policies governing the:

(i) Acquisition of equipment, software, and technology-related services;

(ii) Disposition of equipment;

(iii) Licensing of the radio spectrum by or on behalf of state agencies; and

(iv) Confidentiality of computerized data;

(b) To develop statewide and interagency technical policies, standards, and procedures;

(c) To review and approve standards and common specifications for new or expanded telecommunications networks proposed by agencies, public postsecondary education institutions, educational service districts, or statewide or regional providers of K-12 information technology services;

(d) With input from the legislature and the judiciary, to provide direction concerning strategic planning goals and objectives for the state;

(e) To establish policies for the periodic review by the director of state agency performance which may include but are not limited to analysis of:

(i) Planning, management, control, and use of information services;

(ii) Training and education;

(iii) Project management; and

(iv) Cybersecurity, in coordination with the chief information security officer;

(f) To coordinate with state agencies with an annual information technology expenditure that exceeds ten million dollars to implement a technology business management program to identify opportunities for savings and efficiencies in information technology expenditures and to monitor ongoing financial performance of technology investments;

(g) In conjunction with the consolidated technology services agency, to develop statewide standards for agency purchases of technology networking equipment and services;

(h) To implement a process for detecting, reporting, and responding to security incidents consistent with the information security standards, policies, and guidelines adopted by the director;

(i) To develop plans and procedures to ensure the continuity of commerce for information resources that support the operations and assets of state agencies in the event of a security incident; and

(j) To work with the office of cybersecurity, department of commerce, and other economic development stakeholders to facilitate the development of a strategy that includes key local, state, and federal assets that will create Washington as a national leader in cybersecurity. The office shall collaborate with, including but not limited to, community colleges, universities, the national guard, the department of defense, the department of energy, and national laboratories to develop the strategy.

(3) Statewide technical standards to promote and facilitate electronic information sharing and access are an essential component of acceptable and reliable public access service and complement content-related standards designed to meet those goals. The office shall:

(a) Establish technical standards to facilitate electronic access to government information and interoperability of information systems, including wireless communications systems; and

(b) Require agencies to include an evaluation of electronic public access needs when planning new information systems or major upgrades of systems.

In developing these standards, the office is encouraged to include the state library, state archives, and appropriate representatives of state and local government.

**Sec.**  RCW 43.105.057 and 2011 1st sp.s. c 43 s 807 are each amended to read as follows:

The ((~~agency~~)) office of cybersecurity shall adopt rules as necessary under chapter 34.05 RCW to implement the provisions of this chapter.

**Sec.**  RCW 43.105.060 and 2011 1st sp.s. c 43 s 808 are each amended to read as follows:

State and local government agencies are authorized to enter into any contracts with the ((~~agency~~)) office of cybersecurity which may be necessary or desirable to effectuate the purposes and policies of this chapter or for maximum ((~~utilization~~)) use of facilities and services which are the subject of this chapter.

**Sec.**  RCW 43.105.111 and 2015 3rd sp.s. c 1 s 105 are each amended to read as follows:

The ((~~director~~)) chief information security officer shall set performance targets and approve plans for achieving measurable and specific goals for the ((~~agency~~)) office of cybersecurity. By January 2017, the appropriate organizational performance and accountability measures and performance targets shall be submitted to the governor. These measures and targets shall include measures of performance demonstrating specific and measurable improvements related to service delivery and costs, operational efficiencies, and overall customer satisfaction. The ((~~agency~~)) office of cybersecurity shall develop a dashboard of key performance measures that will be updated quarterly and made available on the ((~~agency~~)) office of cybersecurity public website.

The ((~~director~~)) chief information security officer shall report to the governor on ((~~agency~~)) its performance at least quarterly. The reports shall be included on the ((~~agency's~~)) office of cybersecurity's website and accessible to the public.

**Sec.**  RCW 43.105.225 and 2015 3rd sp.s. c 1 s 204 are each amended to read as follows:

Management of information technology across state government requires managing resources and business processes across multiple agencies. It is no longer sufficient to pursue efficiencies within agency or individual business process boundaries. The state must manage the business process changes and information technology in support of business processes as a statewide portfolio. The ((~~director~~)) chief information security officer will use agency information technology portfolio planning as input to develop a statewide portfolio to guide resource allocation and prioritization decisions.

**Sec.**  RCW 43.105.235 and 2015 3rd sp.s. c 1 s 206 are each amended to read as follows:

(1) Each state agency shall develop an information technology portfolio consistent with RCW 43.105.341. The superintendent of public instruction shall develop its portfolio in conjunction with educational service districts and statewide or regional providers of K-12 education information technology services.

(2) The ((~~director~~)) chief information security officer may exempt any state agency from any or all of the requirements of this section.

**Sec.**  RCW 43.105.245 and 2015 3rd sp.s. c 1 s 208 are each amended to read as follows:

(1) The office shall establish standards and policies governing the planning, implementation, and evaluation of major information technology projects, including those proposed by the superintendent of public instruction, in conjunction with educational service districts, or statewide or regional providers of K-12 education information technology services. The standards and policies shall:

(a) Establish criteria to identify projects which are subject to this section. Such criteria shall include, but not be limited to, significant anticipated cost, complexity, or statewide significance of the project; and

(b) Establish a model process and procedures which state agencies shall follow in developing and implementing projects within their information technology portfolios. This process may include project oversight experts or panels, as appropriate. State agencies may propose, for approval by the office, a process and procedures unique to the agency. The office may accept or require modification of such agency proposals or the office may reject those proposals and require use of the model process and procedures established under this subsection. Any process and procedures developed under this subsection shall require (i) distinct and identifiable phases upon which funding may be based, (ii) user validation of products through system demonstrations and testing of prototypes and deliverables, and (iii) other elements identified by the office.

The ((~~director~~)) chief information security officer may suspend or terminate a major project, and direct that the project funds be placed into unallotted reserve status, if the ((~~director~~)) chief information security officer determines that the project is not meeting or is not expected to meet anticipated performance standards.

(2) The office of financial management shall establish policies and standards consistent with portfolio-based information technology management to govern the funding of projects developed under this section. The policies and standards shall provide for:

(a) Funding of a project under terms and conditions mutually agreed to by the director, the director of financial management, and the head of the agency proposing the project. However, the office of financial management may require incremental funding of a project on a phase-by-phase basis whereby funds for a given phase of a project may be released only when the office of financial management determines, with the advice of the ((~~director~~)) chief information security officer, that the previous phase is satisfactorily completed; and

(b) Other elements deemed necessary by the office of financial management.

**Sec.**  RCW 43.105.255 and 2015 3rd sp.s. c 1 s 209 are each amended to read as follows:

(1) Prior to making a commitment to purchase, acquire, or develop a major information technology project or service, state agencies must provide a proposal to the office outlining the business case of the proposed product or service, including the up-front and ongoing cost of the proposal.

(2) Within thirty days of receipt of a proposal, the office shall approve the proposal, reject it, or propose modifications.

(3) In reviewing a proposal, the office must determine whether the product or service is consistent with:

(a) The standards and policies developed by the ((~~director~~)) office of cybersecurity pursuant to RCW 43.105.054; and

(b) The state's enterprise-based strategy.

(4) If a substantially similar product or service is offered by the ((~~agency~~)) office of cybersecurity, the ((~~director~~)) chief information security officer may require the state agency to procure the product or service through the ((~~agency~~)) office of cybersecurity, if doing so would benefit the state as an enterprise.

(5) The office shall provide guidance to state agencies as to what threshold of information technology spending constitutes a major information technology product or service under this section.

**Sec.**  RCW 43.88.090 and 2015 3rd sp.s. c 1 s 409 are each amended to read as follows:

(1) For purposes of developing budget proposals to the legislature, the governor shall have the power, and it shall be the governor's duty, to require from proper agency officials such detailed estimates and other information in such form and at such times as the governor shall direct. The governor shall communicate statewide priorities to state agencies for use in developing biennial budget recommendations for their agency and shall seek public involvement and input on these priorities. The estimates for the legislature and the judiciary shall be transmitted to the governor and shall be included in the budget without revision. The estimates for state pension contributions shall be based on the rates provided in chapter 41.45 RCW. Copies of all such estimates shall be transmitted to the standing committees on ways and means of the house and senate at the same time as they are filed with the governor and the office of financial management.

The estimates shall include statements or tables which indicate, by agency, the state funds which are required for the receipt of federal matching revenues. The estimates shall be revised as necessary to reflect legislative enactments and adopted appropriations and shall be included with the initial biennial allotment submitted under RCW 43.88.110. The estimates must reflect that the agency considered any alternatives to reduce costs or improve service delivery identified in the findings of a performance audit of the agency by the joint legislative audit and review committee. Nothing in this subsection requires performance audit findings to be published as part of the budget.

(2) Each state agency shall define its mission and establish measurable goals for achieving desirable results for those who receive its services and the taxpayers who pay for those services. Each agency shall also develop clear strategies and timelines to achieve its goals. This section does not require an agency to develop a new mission or goals in place of identifiable missions or goals that meet the intent of this section. The mission and goals of each agency must conform to statutory direction and limitations.

(3) For the purpose of assessing activity performance, each state agency shall establish quality and productivity objectives for each major activity in its budget. The objectives must be consistent with the missions and goals developed under this section. The objectives must be expressed to the extent practicable in outcome-based, objective, and measurable form unless an exception to adopt a different standard is granted by the office of financial management and approved by the legislative committee on performance review. Objectives must specifically address the statutory purpose or intent of the program or activity and focus on data that measure whether the agency is achieving or making progress toward the purpose of the activity and toward statewide priorities. The office of financial management shall provide necessary professional and technical assistance to assist state agencies in the development of strategic plans that include the mission of the agency and its programs, measurable goals, strategies, and performance measurement systems.

(4) Each state agency shall adopt procedures for and perform continuous self-assessment of each activity, using the mission, goals, objectives, and measurements required under subsections (2) and (3) of this section. The assessment of the activity must also include an evaluation of major information technology systems or projects that may assist the agency in achieving or making progress toward the activity purpose and statewide priorities. The evaluation of proposed major information technology systems or projects shall be in accordance with the standards and policies established by the technology services board. Agencies' progress toward the mission, goals, objectives, and measurements required by subsections (2) and (3) of this section is subject to review as set forth in this subsection.

(a) The office of financial management shall regularly conduct reviews of selected activities to analyze whether the objectives and measurements submitted by agencies demonstrate progress toward statewide results.

(b) The office of financial management shall consult with: (i) The four-year institutions of higher education in those reviews that involve four-year institutions of higher education; and (ii) the state board for community and technical colleges in those reviews that involve two-year institutions of higher education.

(c) The goal is for all major activities to receive at least one review each year.

(d) The ((~~consolidated technology services agency~~)) office of cybersecurity shall periodically review major information technology systems ((~~in use~~)) used by state agencies ((~~periodically~~)).

(5) It is the policy of the legislature that each agency's budget recommendations must be directly linked to the agency's stated mission and program, quality, and productivity goals and objectives. Consistent with this policy, agency budget proposals must include integration of performance measures that allow objective determination of an activity's success in achieving its goals. When a review under subsection (4) of this section or other analysis determines that the agency's objectives demonstrate that the agency is making insufficient progress toward the goals of any particular program or is otherwise underachieving or inefficient, the agency's budget request shall contain proposals to remedy or improve the selected programs. The office of financial management shall develop a plan to merge the budget development process with agency performance assessment procedures. The plan must include a schedule to integrate agency strategic plans and performance measures into agency budget requests and the governor's budget proposal over three fiscal biennia. The plan must identify those agencies that will implement the revised budget process in the 1997-1999 biennium, the 1999-2001 biennium, and the 2001-2003 biennium. In consultation with the legislative fiscal committees, the office of financial management shall recommend statutory and procedural modifications to the state's budget, accounting, and reporting systems to facilitate the performance assessment procedures and the merger of those procedures with the state budget process. The plan and recommended statutory and procedural modifications must be submitted to the legislative fiscal committees by September 30, 1996.

(6) In reviewing agency budget requests in order to prepare the governor's biennial budget request, the office of financial management shall consider the extent to which the agency's activities demonstrate progress toward the statewide budgeting priorities, along with any specific review conducted under subsection (4) of this section.

(7) In the year of the gubernatorial election, the governor shall invite the governor-elect or the governor-elect's designee to attend all hearings provided in RCW 43.88.100; and the governor shall furnish the governor-elect or the governor-elect's designee with such information as will enable the governor-elect or the governor-elect's designee to gain an understanding of the state's budget requirements. The governor-elect or the governor-elect's designee may ask such questions during the hearings and require such information as the governor-elect or the governor-elect's designee deems necessary and may make recommendations in connection with any item of the budget which, with the governor-elect's reasons therefor, shall be presented to the legislature in writing with the budget document. Copies of all such estimates and other required information shall also be submitted to the standing committees on ways and means of the house and senate.

**Sec.**  RCW 43.105.287 and 2015 3rd sp.s. c 1 s 212 are each amended to read as follows:

The board shall have the following powers and duties related to information services:

(1) To review and approve standards and policies, developed by the office, governing the acquisition and disposition of equipment, proprietary software, and purchased services, licensing of the radio spectrum by or on behalf of state agencies, and confidentiality of computerized data;

(2) To review and approve statewide or interagency technical policies and standards developed by the office;

(3) To review, approve, and provide oversight of major information technology projects to ensure that no major information technology project proposed by a state agency is approved or authorized funding by the board without consideration of the technical and financial business case for the project, including a review of:

(a) The total cost of ownership across the life of the project;

(b) All major technical options and alternatives analyzed, and reviewed, if necessary, by independent technical sources; and

(c) Whether the project is technically and financially justifiable when compared against the state's enterprise-based strategy, long-term technology trends, and existing or potential partnerships with private providers or vendors;

(4) To review and approve standards and common specifications for new or expanded telecommunications networks proposed by state agencies, public postsecondary education institutions, educational service districts, or statewide or regional providers of K-12 information technology services, and to assure the cost-effective development and incremental implementation of a statewide video telecommunications system to serve: Public schools; educational service districts; vocational-technical institutes; community colleges; colleges and universities; state and local government; and the general public through public affairs programming;

(5) To develop a policy to determine whether a proposed project, product, or service should undergo an independent technical and financial analysis prior to submitting a request to the office of financial management for the inclusion in any proposed operating, capital, or transportation budget;

(6) To approve contracting for services and activities under RCW 41.06.142((~~(7)~~)) (11) for the ((~~agency~~)) office of cybersecurity. To approve any service or activity to be contracted under RCW 41.06.142((~~(7)(b)~~)) (11), the board must also review the proposed business plan and recommendation submitted by the office;

(7) To consider, on an ongoing basis, ways to promote strategic investments in enterprise-level information technology projects that will result in service improvements and cost efficiency;

(8) To provide a forum to solicit external expertise and perspective on developments in information technology, enterprise architecture, standards, and policy development; ((~~and~~))

(9) To provide a forum where ideas and issues related to information technology plans, policies, and standards can be reviewed; and

(10) To review and approve standards and policies developed by the office of cybersecurity, pursuant to section 1 of this act, governing the protection and oversight of the state's information technology systems and infrastructure and cybersecurity prevention and response protocols.

**Sec.**  RCW 41.06.142 and 2020 c 269 s 2 are each amended to read as follows:

(1) If any department, agency, or institution of higher education intends to contract for services that, on or after July 1, 2005, have been customarily and historically provided by, and would displace or relocate, employees in the classified service under this chapter, a department, agency, or institution of higher education may do so by contracting with individuals, nonprofit organizations, businesses, employee business units, or other entities if the following criteria are met:

(a) A comprehensive impact assessment is completed by the agency, department, or institution of higher education to assist it in determining whether the decision to contract out is beneficial.

(i) The comprehensive impact assessment must include at a minimum the following analysis:

(A) An estimate of the cost of performance of the service by employees, including the fully allocated costs of the service, the cost of the employees' salaries and benefits, space, equipment, materials, and other costs necessary to perform the function. The estimate must not include the state's indirect overhead costs unless those costs can be attributed directly to the function in question and would not exist if that function were not performed in state service;

(B) An estimate of the cost of performance of the services if contracted out, including the cost of administration of the program and allocating sufficient employee staff time and resources to monitor the contract and ensure its proper performance by the contractor;

(C) The reason for proposing to contract out, including the objective the agency would like to achieve; and

(D) The reasons for the determination made under (e) of this subsection.

(ii) When the contract will result in termination of state employees or elimination of state positions, the comprehensive impact assessment may also include an assessment of the potential adverse impacts on the public from outsourcing the contract, such as loss of employment, effect on social services and public assistance programs, economic impacts on local businesses and local tax revenues, and environmental impacts;

(b) The invitation for bid or request for proposal contains measurable standards for the performance of the contract;

(c) Employees whose positions or work would be displaced by the contract are provided an opportunity to offer alternatives to purchasing services by contract and, if these alternatives are not accepted, compete for the contract under competitive contracting procedures in subsection (7) of this section;

(d) The department, agency, or institution of higher education has established a contract monitoring process to measure contract performance, costs, service delivery quality, and other contract standards, and to cancel contracts that do not meet those standards; and

(e) The department, agency, or institution of higher education has determined that the contract results in savings or efficiency improvements. The contracting agency, department, or institution of higher education must consider the consequences and potential mitigation of improper or failed performance by the contractor.

(2)(a) The agency, department, or institution of higher education must post on its website the request for proposal, the contract or a statement that the agency, department, or institution of higher education did not move forward with contracting out, and the comprehensive impact assessment pursuant to subsection (1) of this section.

(b) The agency, department, or institution of higher education must maintain the information in (a) of this subsection in its files in accordance with the record retention schedule under RCW 40.14.060.

(3) Every five years or upon completion of the contract, whichever comes first, the agency, department, or institution of higher education must prepare and maintain in the contract file a report, which must include at a minimum the following information:

(a) Documentation of the contractor's performance as measured by the itemized performance standards;

(b) Itemization of any contract extensions or change orders that resulted in a change in the dollar value or cost of the contract; and

(c) A report of any remedial actions that were taken to enforce compliance with the contract, together with an estimate of the cost incurred by the agency, department, or institution of higher education in enforcing such compliance.

(4) In addition to any other terms required by law, the terms of any agreement to contract out a service pursuant to this section must include terms that address the following:

(a) The contract's contract management provision must allow review of the contractor's performance;

(b) The contract's termination clauses must allow termination of the contract if the contractor fails to meet the terms of the contract, including failure to meet performance standards or failure to provide the services at the contracted price;

(c) The contract's damages provision must allow recovery of direct damages and**,** when applicable, indirect damages that the agency, department, or institution of higher education incurs due to the contractor's breach of the agreement;

(d) If the contractor will be using a subcontractor for performance of services under the contract, the contract must allow the agency, department, or institution of higher education to obtain information about the subcontractor, as applicable to the performance of services under the agreement; and

(e) A provision requiring the contractor to consider employment of employees who may be displaced by the contract, if the contract is with an entity other than an employee business unit.

(5) Any provision contrary to or in conflict with this section in any collective bargaining agreement in effect on July 1, 2005, is not effective beyond the expiration date of the agreement.

(6) When contracting out for services as authorized in this section the agency, department, or institution of higher education must ensure firms adhere to the values of the state of Washington under RCW 49.60.030, which provide its citizens freedom from discrimination. Any relationship with a potential or current industry partner that is found to have violated RCW 49.60.030 by the attorney general shall not be considered and must be immediately terminated unless:

(a) The industry partner has fulfilled the conditions or obligations associated with any court order or settlement resulting from that violation; or

(b) The industry partner has taken significant and meaningful steps to correct the violation, as determined by the Washington state human rights commission.

(7) Competitive contracting shall be implemented as follows:

(a) At least ninety days prior to the date the contracting agency, department, or institution of higher education requests bids from private entities for a contract for services provided by employees, the contracting agency, department, or institution of higher education shall notify the employees whose positions or work would be displaced by the contract. The employees shall have sixty days from the date of notification to offer alternatives to purchasing services by contract, and the agency, department, or institution of higher education shall consider the alternatives before requesting bids.

(b) If the employees decide to compete for the contract, they shall notify the contracting agency, department, or institution of higher education of their decision. Employees must form one or more employee business units for the purpose of submitting a bid or bids to perform the services.

(c) The department of enterprise services, with the advice and assistance of the office of financial management, shall develop and make available to employee business units training in the bidding process and general bid preparation.

(d) The director of enterprise services, with the advice and assistance of the office of financial management, shall, by rule, establish procedures to ensure that bids are submitted and evaluated in a fair and objective manner and that there exists a competitive market for the service. Such rules shall include, but not be limited to: (i) Prohibitions against participation in the bid evaluation process by employees who prepared the business unit's bid or who perform any of the services to be contracted; (ii) provisions to ensure no bidder receives an advantage over other bidders and that bid requirements are applied equitably to all parties; and (iii) procedures that require the contracting agency, department, or institution of higher education to receive complaints regarding the bidding process and to consider them before awarding the contract. Appeal of an agency's, department's, or institution of higher education's actions under this subsection is an adjudicative proceeding and subject to the applicable provisions of chapter 34.05 RCW, the administrative procedure act, with the final decision to be rendered by an administrative law judge assigned under chapter 34.12 RCW.

(e) An employee business unit's bid must include the fully allocated costs of the service, including the cost of the employees' salaries and benefits, space, equipment, materials, and other costs necessary to perform the function. An employee business unit's cost shall not include the state's indirect overhead costs unless those costs can be attributed directly to the function in question and would not exist if that function were not performed in state service.

(f) A department, agency, or institution of higher education may contract with the department of enterprise services to conduct the bidding process.

(8)(a) As used in this section:

(i) "Employee business unit" means a group of employees who perform services to be contracted under this section and who submit a bid for the performance of those services under subsection (7) of this section.

(ii) "Indirect overhead costs" means the pro rata share of existing agency administrative salaries and benefits, and rent, equipment costs, utilities, and materials associated with those administrative functions.

(iii) "Competitive contracting" means the process by which employees of a department, agency, or institution of higher education compete with businesses, individuals, nonprofit organizations, or other entities for contracts authorized by subsection (1) of this section.

(b) Unless otherwise specified, for the purpose of chapter 269, Laws of 2020, "employee" means state employees in the classified service under this chapter except employees in the Washington management service as defined under RCW 41.06.022 and 41.06.500.

(9) The processes set forth in subsections (1)(a), (2), (3), and (4)(a) through (d) of this section do not apply to contracts:

(a) Awarded for the purposes of or by the department of transportation;

(b) With an estimated cost of contract performance of twenty thousand dollars or less;

(c) With an estimated cost of contract performance that exceeds five hundred thousand dollars for public work as defined by RCW 39.04.010; or

(d) Relating to mechanical, plumbing as described in chapter 18.106 RCW, and electrical as described in chapter 19.28 RCW, procured to install systems for new construction or life-cycle replacement with an estimated cost of contract performance of seventy-five thousand dollars or more.

(10) The processes set forth in subsections (1) through (4), (7), and (8) of this section do not apply to:

(a) RCW 74.13.031(6);

(b) The acquisition of printing services by a state agency; and

(c) Contracts for services expressly mandated by the legislature, including contracts for fire suppression awarded by the department of natural resources under RCW 76.04.181, or authorized by law prior to July 1, 2005, including contracts and agreements between public entities.

(11) The processes set forth in subsections (1) through (4), (7), and (8) of this section do not apply to the ((~~consolidated technology services agency~~)) office of cybersecurity when contracting for services or activities as follows:

(a) Contracting for services and activities that are necessary to establish, operate, or manage the state data center, including architecture, design, engineering, installation, and operation of the facility that are approved by the technology services board created in RCW 43.105.285.

(b) Contracting for services and activities recommended by the chief information security officer through a business plan and approved by the technology services board created in RCW 43.105.285.

**Sec.**  RCW 43.105.342 and 2015 3rd sp.s. c 1 s 501 are each amended to read as follows:

(1) The ((~~consolidated technology services~~)) office of cybersecurity and information oversight revolving account is created in the custody of the state treasurer. All receipts from ((~~agency~~)) fees and charges for services collected by the office of cybersecurity and information oversight from public agencies must be deposited into the account. The account must be used for the:

(a) Acquisition of equipment, software, supplies, and services; and

(b) Payment of salaries, wages, and other costs incidental to the acquisition, development, maintenance, operation, and administration of: (i) Information services; (ii) telecommunications; (iii) systems; (iv) software; (v) supplies; and (vi) equipment, including the payment of principal and interest on debt by the agency and other users as determined by the office of financial management.

(2) The ((~~director or the director's~~)) chief information security officer or his or her designee, with the approval of the technology services board, is authorized to expend up to one million dollars per fiscal biennium for the technology services board to conduct independent technical and financial analysis of proposed information technology projects.

(3) Only the ((~~director or the director's~~)) chief information security officer or his or her designee may authorize expenditures from the account. The account is subject to allotment procedures under chapter 43.88 RCW, but no appropriation is required for expenditures except as provided in subsection (4) of this section.

(4) Expenditures for the strategic planning and policy component of the agency are subject to appropriation.

**Sec.**  RCW 43.105.369 and 2016 c 195 s 2 are each amended to read as follows:

(1) The office of privacy and data protection is created within the office of the state chief information officer. The purpose of the office of privacy and data protection is to serve as a central point of contact for state agencies on policy matters involving data privacy and data protection.

(2) The ((~~director~~)) chief information security officer shall appoint the chief privacy officer, who is the director of the office of privacy and data protection.

(3) The primary duties of the office of privacy and data protection with respect to state agencies are:

(a) To conduct an annual privacy review;

(b) To conduct an annual privacy training for state agencies and employees;

(c) To articulate privacy principles and best practices;

(d) To coordinate data protection in cooperation with the agency; and

(e) To participate with the office of the state chief information officer in the review of major state agency projects involving personally identifiable information.

(4) The office of privacy and data protection must serve as a resource to local governments and the public on data privacy and protection concerns by:

(a) Developing and promoting the dissemination of best practices for the collection and storage of personally identifiable information, including establishing and conducting a training program or programs for local governments; and

(b) Educating consumers about the use of personally identifiable information on mobile and digital networks and measures that can help protect this information.

(5) By December 1, 2016, and every four years thereafter, the office of privacy and data protection must prepare and submit to the legislature a report evaluating its performance. The office of privacy and data protection must establish performance measures in its 2016 report to the legislature and, in each report thereafter, demonstrate the extent to which performance results have been achieved. These performance measures must include, but are not limited to, the following:

(a) The number of state agencies and employees who have participated in the annual privacy training;

(b) A report on the extent of the office of privacy and data protection's coordination with international and national experts in the fields of data privacy, data protection, and access equity;

(c) A report on the implementation of data protection measures by state agencies attributable in whole or in part to the office of privacy and data protection's coordination of efforts; and

(d) A report on consumer education efforts, including but not limited to the number of consumers educated through public outreach efforts, as indicated by how frequently educational documents were accessed, the office of privacy and data protection's participation in outreach events, and inquiries received back from consumers via telephone or other media.

(6) Within one year of June 9, 2016, the office of privacy and data protection must submit to the joint legislative audit and review committee for review and comment the performance measures developed under subsection (5) of this section and a data collection plan.

(7) The office of privacy and data protection shall submit a report to the legislature on the: (a) Extent to which telecommunications providers in the state are deploying advanced telecommunications capability; and (b) existence of any inequality in access to advanced telecommunications infrastructure experienced by residents of tribal lands, rural areas, and economically distressed communities. The report may be submitted at a time within the discretion of the office of privacy and data protection, at least once every four years, and only to the extent the office of privacy and data protection is able to gather and present the information within existing resources.

**Sec.**  RCW 43.105.385 and 2015 3rd sp.s. c 1 s 220 are each amended to read as follows:

(1) The office shall conduct a needs assessment and develop a migration strategy to ensure that, over time, all state agencies are moving towards using the ((~~agency~~)) office of cybersecurity as their central service provider for all utility-based infrastructure services, including centralized PC and infrastructure support. State agency-specific application services shall remain managed within individual agencies.

(2) The office shall develop short-term and long-term objectives as part of the migration strategy.

(3) This section does not apply to institutions of higher education.

**Sec.**  RCW 43.105.905 and 2008 c 262 s 4 are each amended to read as follows:

Nothing in this act may be construed as giving the ((~~department of information services~~)) office of cybersecurity or any other entities any additional authority, regulatory or otherwise, over providers of telecommunications and information technology.

**Sec.**  RCW 43.105.907 and 2011 1st sp.s. c 43 s 1009 are each amended to read as follows:

(1) Those powers, duties, and functions of the department of information services being transferred to the consolidated technology services agency as set forth in sections 801 through 816, chapter 43, Laws of 2011 1st sp. sess. are hereby transferred to the consolidated technology services agency, unless otherwise specified under chapter . . ., Laws of 2021 (this act).

(2)(a) All reports, documents, surveys, books, records, files, papers, or written material in the possession of the department of information services shall be delivered to the custody of the consolidated technology services agency. All cabinets, furniture, office equipment, motor vehicles, and other tangible property employed by the department of information services shall be made available to the consolidated technology services agency. All funds, credits, or other assets held by the department of information services shall be assigned to the consolidated technology services agency.

(b) Any appropriations made to the department of information services shall, on October 1, 2011, be transferred and credited to the consolidated technology services agency.

(c) If any question arises as to the transfer of any personnel, funds, books, documents, records, papers, files, equipment, or other tangible property used or held in the exercise of the powers and the performance of the duties and functions transferred, the director of financial management shall make a determination as to the proper allocation and certify the same to the state agencies concerned.

(3) Unless otherwise provided under chapter . . ., Laws of 2021 (this act):

(a) All rules and all pending business before the department of information services pertaining to the powers, duties, and functions transferred shall be continued and acted upon by the consolidated technology services agency((~~.~~)); and

(b) All existing contracts and obligations shall remain in full force and shall be performed by the consolidated technology services agency.

(4) The transfer of the powers, duties, functions, and personnel of the department of information services shall not affect the validity of any act performed before October 1, 2011.

(5) If apportionments of budgeted funds are required because of the transfers directed by this section, the director of financial management shall certify the apportionments to the agencies affected, the state auditor, and the state treasurer. Each of these shall make the appropriate transfer and adjustments in funds and appropriation accounts and equipment records in accordance with the certification.

(6) All employees of the department of information services engaged in performing the powers, functions, and duties transferred to the consolidated technology services agency or otherwise to the office of cybersecurity are transferred to the ((~~consolidated technology services agency~~)) office of cybersecurity. All employees classified under chapter 41.06 RCW, the state civil service law, are assigned to the ((~~consolidated technology services agency~~)) office of cybersecurity to perform their usual duties upon the same terms as formerly, without any loss of rights, subject to any action that may be appropriate thereafter in accordance with the laws and rules governing state civil service law.

(7) Unless or until modified by the public employment relations commission pursuant to RCW 41.80.911:

(a) The portions of the bargaining units of employees at the department of information services existing on October 1, 2011, shall be considered appropriate units at the ((~~consolidated technology services agency~~)) office of cybersecurity and will be so certified by the public employment relations commission.

(b) The exclusive bargaining representatives recognized as representing the portions of the bargaining units of employees at the department of information services existing on October 1, 2011, shall continue as the exclusive bargaining representatives of the transferred bargaining units without the necessity of an election.

**Sec.**  RCW 39.26.100 and 2019 c 152 s 2 are each amended to read as follows:

(1) The provisions of this chapter do not apply in any manner to the operation of the state legislature except as requested by the legislature.

(2) The provisions of this chapter do not apply to the contracting for services, equipment, and activities that are necessary to establish, operate, or manage the state data center, including architecture, design, engineering, installation, and operation of the facility, that are approved by the technology services board or the acquisition of proprietary software, equipment, and information technology services necessary for or part of the provision of services offered by the ((~~consolidated technology services agency~~)) office of cybersecurity and information oversight.

(3) Primary authority for the purchase of specialized equipment, and instructional and research material, for their own use rests with the institutions of higher education as defined in RCW 28B.10.016.

(4) Universities operating hospitals with approval from the director, as the agent for state hospitals as defined in RCW 72.23.010, and for health care programs provided in state correctional institutions as defined in RCW 72.65.010(3) and veterans' institutions as defined in RCW 72.36.010 and 72.36.070, may make purchases for hospital operation by participating in contracts for materials, supplies, and equipment entered into by nonprofit cooperative hospital group purchasing organizations if documented to be more cost-effective.

(5) Primary authority for the purchase of materials, supplies, and equipment, for resale to other than public agencies, rests with the state agency concerned.

(6) The authority for the purchase of insurance and bonds rests with the risk manager under RCW 43.19.769, except for institutions of higher education that choose to exercise independent purchasing authority under RCW 28B.10.029.

(7) The provisions of this chapter do not apply to information technology purchases by state agencies, other than institutions of higher education and agencies of the judicial branch, if (a) the purchase is less than one hundred thousand dollars, (b) the initial purchase is approved by the ((~~chief information officer of the state~~)) chief information security officer, and (c) the agency director and the chief information security officer ((~~of the state~~)) jointly prepare a public document providing a detailed justification for the expenditure.

(8) The authority to purchase interpreter services on behalf of applicants and recipients of public assistance who are sensory-impaired rests with the department of social and health services and the health care authority.

**Sec.**  RCW 41.06.070 and 2019 c 146 s 3 are each amended to read as follows:

(1) The provisions of this chapter do not apply to:

(a) The members of the legislature or to any employee of, or position in, the legislative branch of the state government including members, officers, and employees of the legislative council, joint legislative audit and review committee, statute law committee, and any interim committee of the legislature;

(b) The justices of the supreme court, judges of the court of appeals, judges of the superior courts or of the inferior courts, or to any employee of, or position in the judicial branch of state government;

(c) Officers, academic personnel, and employees of technical colleges;

(d) The officers of the Washington state patrol;

(e) Elective officers of the state;

(f) The chief executive officer of each agency;

(g) In the departments of employment security and social and health services, the director and the director's confidential secretary; in all other departments, the executive head of which is an individual appointed by the governor, the director, his or her confidential secretary, and his or her statutory assistant directors;

(h) In the case of a multimember board, commission, or committee, whether the members thereof are elected, appointed by the governor or other authority, serve ex officio, or are otherwise chosen:

(i) All members of such boards, commissions, or committees;

(ii) If the members of the board, commission, or committee serve on a part-time basis and there is a statutory executive officer: The secretary of the board, commission, or committee; the chief executive officer of the board, commission, or committee; and the confidential secretary of the chief executive officer of the board, commission, or committee;

(iii) If the members of the board, commission, or committee serve on a full-time basis: The chief executive officer or administrative officer as designated by the board, commission, or committee; and a confidential secretary to the chair of the board, commission, or committee;

(iv) If all members of the board, commission, or committee serve ex officio: The chief executive officer; and the confidential secretary of such chief executive officer;

(i) The confidential secretaries and administrative assistants in the immediate offices of the elective officers of the state;

(j) Assistant attorneys general;

(k) Commissioned and enlisted personnel in the military service of the state;

(l) Inmate, student, and temporary employees, and part-time professional consultants, as defined by the director;

(m) Officers and employees of the Washington state fruit commission;

(n) Officers and employees of the Washington apple commission;

(o) Officers and employees of the Washington state dairy products commission;

(p) Officers and employees of the Washington tree fruit research commission;

(q) Officers and employees of the Washington state beef commission;

(r) Officers and employees of the Washington grain commission;

(s) Officers and employees of any commission formed under chapter 15.66 RCW;

(t) Officers and employees of agricultural commissions formed under chapter 15.65 RCW;

(u) Executive assistants for personnel administration and labor relations in all state agencies employing such executive assistants including but not limited to all departments, offices, commissions, committees, boards, or other bodies subject to the provisions of this chapter and this subsection shall prevail over any provision of law inconsistent herewith unless specific exception is made in such law;

(v) In each agency with fifty or more employees: Deputy agency heads, assistant directors or division directors, and not more than three principal policy assistants who report directly to the agency head or deputy agency heads;

(w) Staff employed by the department of commerce to administer energy policy functions;

(x) The manager of the energy facility site evaluation council;

(y) A maximum of ten staff employed by the department of commerce to administer innovation and policy functions, including the three principal policy assistants exempted under (v) of this subsection;

(z) Staff employed by Washington State University to administer energy education, applied research, and technology transfer programs under RCW 43.21F.045 as provided in RCW 28B.30.900(5);

(aa) Officers and employees of the ((~~consolidated technology services agency created in RCW 43.105.006~~)) office of cybersecurity and information oversight established under section 1 of this act that perform the following functions or duties: Systems integration; data center engineering and management; network systems engineering and management; information technology contracting; information technology customer relations management; and network and systems security;

(bb) The executive director of the Washington statewide reentry council.

(2) The following classifications, positions, and employees of institutions of higher education and related boards are hereby exempted from coverage of this chapter:

(a) Members of the governing board of each institution of higher education and related boards, all presidents, vice presidents, and their confidential secretaries, administrative, and personal assistants; deans, directors, and chairs; academic personnel; and executive heads of major administrative or academic divisions employed by institutions of higher education; principal assistants to executive heads of major administrative or academic divisions; other managerial or professional employees in an institution or related board having substantial responsibility for directing or controlling program operations and accountable for allocation of resources and program results, or for the formulation of institutional policy, or for carrying out personnel administration or labor relations functions, legislative relations, public information, development, senior computer systems and network programming, or internal audits and investigations; and any employee of a community college district whose place of work is one which is physically located outside the state of Washington and who is employed pursuant to RCW 28B.50.092 and assigned to an educational program operating outside of the state of Washington;

(b) The governing board of each institution, and related boards, may also exempt from this chapter classifications involving research activities, counseling of students, extension or continuing education activities, graphic arts or publications activities requiring prescribed academic preparation or special training as determined by the board: PROVIDED, That no nonacademic employee engaged in office, clerical, maintenance, or food and trade services may be exempted by the board under this provision;

(c) Printing craft employees in the department of printing at the University of Washington.

(3) In addition to the exemptions specifically provided by this chapter, the director may provide for further exemptions pursuant to the following procedures. The governor or other appropriate elected official may submit requests for exemption to the office of financial management stating the reasons for requesting such exemptions. The director shall hold a public hearing, after proper notice, on requests submitted pursuant to this subsection. If the director determines that the position for which exemption is requested is one involving substantial responsibility for the formulation of basic agency or executive policy or one involving directing and controlling program operations of an agency or a major administrative division thereof, or is a senior expert in enterprise information technology infrastructure, engineering, or systems, the director shall grant the request. The total number of additional exemptions permitted under this subsection shall not exceed one percent of the number of employees in the classified service not including employees of institutions of higher education and related boards for those agencies not directly under the authority of any elected public official other than the governor, and shall not exceed a total of twenty-five for all agencies under the authority of elected public officials other than the governor.

(4) The salary and fringe benefits of all positions presently or hereafter exempted except for the chief executive officer of each agency, full-time members of boards and commissions, administrative assistants and confidential secretaries in the immediate office of an elected state official, and the personnel listed in subsections (1)(j) through (t) and (2) of this section, shall be determined by the director. Changes to the classification plan affecting exempt salaries must meet the same provisions for classified salary increases resulting from adjustments to the classification plan as outlined in RCW 41.06.152.

(5)(a) Any person holding a classified position subject to the provisions of this chapter shall, when and if such position is subsequently exempted from the application of this chapter, be afforded the following rights: If such person previously held permanent status in another classified position, such person shall have a right of reversion to the highest class of position previously held, or to a position of similar nature and salary.

(b) Any classified employee having civil service status in a classified position who accepts an appointment in an exempt position shall have the right of reversion to the highest class of position previously held, or to a position of similar nature and salary.

(c) A person occupying an exempt position who is terminated from the position for gross misconduct or malfeasance does not have the right of reversion to a classified position as provided for in this section.

**Sec.**  RCW 41.06.094 and 2015 c 225 s 54 are each amended to read as follows:

In addition to the exemptions under RCW 41.06.070, the provisions of this chapter shall not apply in the ((~~consolidated technology services agency~~)) office of cybersecurity and information oversight to up to twelve positions in the planning component involved in policy development and/or senior professionals.

**Sec.**  RCW 42.17A.705 and 2017 3rd sp.s. c 6 s 111 are each amended to read as follows:

For the purposes of RCW 42.17A.700, "executive state officer" includes:

(1) The chief administrative law judge, the director of agriculture, the director of the department of services for the blind, the secretary of children, youth, and families, the director of the state system of community and technical colleges, the director of commerce, the director of the ((~~consolidated technology services agency~~)) office of cybersecurity and information oversight, the secretary of corrections, the director of ecology, the commissioner of employment security, the chair of the energy facility site evaluation council, the director of enterprise services, the secretary of the state finance committee, the director of financial management, the director of fish and wildlife, the executive secretary of the forest practices appeals board, the director of the gambling commission, the secretary of health, the administrator of the Washington state health care authority, the executive secretary of the health care facilities authority, the executive secretary of the higher education facilities authority, the executive secretary of the horse racing commission, the executive secretary of the human rights commission, the executive secretary of the indeterminate sentence review board, the executive director of the state investment board, the director of labor and industries, the director of licensing, the director of the lottery commission, the director of the office of minority and women's business enterprises, the director of parks and recreation, the executive director of the public disclosure commission, the executive director of the Puget Sound partnership, the director of the recreation and conservation office, the director of retirement systems, the director of revenue, the secretary of social and health services, the chief of the Washington state patrol, the executive secretary of the board of tax appeals, the secretary of transportation, the secretary of the utilities and transportation commission, the director of veterans affairs, the president of each of the regional and state universities and the president of The Evergreen State College, and each district and each campus president of each state community college;

(2) Each professional staff member of the office of the governor;

(3) Each professional staff member of the legislature; and

(4) Central Washington University board of trustees, the boards of trustees of each community college and each technical college, each member of the state board for community and technical colleges, state convention and trade center board of directors, Eastern Washington University board of trustees, Washington economic development finance authority, Washington energy northwest executive board, The Evergreen State College board of trustees, executive ethics board, fish and wildlife commission, forest practices appeals board, forest practices board, gambling commission, Washington health care facilities authority, student achievement council, higher education facilities authority, horse racing commission, state housing finance commission, human rights commission, indeterminate sentence review board, board of industrial insurance appeals, state investment board, commission on judicial conduct, legislative ethics board, life sciences discovery fund authority board of trustees, state liquor and cannabis board, lottery commission, Pacific Northwest electric power and conservation planning council, parks and recreation commission, Washington personnel resources board, board of pilotage commissioners, pollution control hearings board, public disclosure commission, public employees' benefits board, recreation and conservation funding board, salmon recovery funding board, shorelines hearings board, board of tax appeals, transportation commission, University of Washington board of regents, utilities and transportation commission, Washington State University board of regents, and Western Washington University board of trustees.

**Sec.**  RCW 43.41.391 and 2015 3rd sp.s. c 1 s 214 are each amended to read as follows:

(1) The office has the duty to govern and oversee the technical design, implementation, and operation of the K-20 network including, but not limited to, the following duties: Establishment and implementation of K-20 network technical policy, including technical standards and conditions of use; review and approval of network design; and resolving user/provider disputes.

(2) The office has the following powers and duties:

(a) In cooperation with the educational sectors and other interested parties, to establish goals and measurable objectives for the network;

(b) To ensure that the goals and measurable objectives of the network are the basis for any decisions or recommendations regarding the technical development and operation of the network;

(c) To adopt, modify, and implement policies to facilitate network development, operation, and expansion. Such policies may include but need not be limited to the following issues: Quality of educational services; access to the network by recognized organizations and accredited institutions that deliver educational programming, including public libraries; prioritization of programming within limited resources; prioritization of access to the system and the sharing of technological advances; network security; identification and evaluation of emerging technologies for delivery of educational programs; future expansion or redirection of the system; network fee structures; and costs for the development and operation of the network;

(d) To prepare and submit to the governor and the legislature a coordinated budget for network development, operation, and expansion. The budget shall include the director of the ((~~consolidated technology services agency's~~)) office of cybersecurity and information oversights' recommendations on (i) any state funding requested for network transport and equipment, distance education facilities and hardware or software specific to the use of the network, and proposed new network end sites, (ii) annual copayments to be charged to public educational sector institutions and other public entities connected to the network, and (iii) charges to nongovernmental entities connected to the network;

(e) To adopt and monitor the implementation of a methodology to evaluate the effectiveness of the network in achieving the educational goals and measurable objectives;

(f) To establish by rule acceptable use policies governing user eligibility for participation in the K-20 network, acceptable uses of network resources, and procedures for enforcement of such policies. The office shall set forth appropriate procedures for enforcement of acceptable use policies, that may include suspension of network connections and removal of shared equipment for violations of network conditions or policies. The office shall have sole responsibility for the implementation of enforcement procedures relating to technical conditions of use.

**Sec.**  RCW 43.41.442 and 2015 3rd sp.s. c 1 s 503 are each amended to read as follows:

(1) The statewide information technology system maintenance and operations revolving account is created in the custody of the state treasurer. All receipts from fees, charges for services, and assessments to agencies for the maintenance and operations of enterprise information technology systems must be deposited into the account. The account must be used solely for the maintenance and operations of enterprise information technology systems.

(2) Only the director or the director's designee may authorize expenditures from the account. The account is subject to allotment procedures under chapter 43.88 RCW, but no appropriation is required for expenditure.

(3) The office may contract with the ((~~consolidated technology services agency~~)) office of cybersecurity and information oversight for the billing of fees, charges for services, and assessments to agencies, and for the maintenance and operations of enterprise information technology systems.

(4) "Enterprise information technology system" has the definition in RCW 43.41.440.

**Sec.**  RCW 43.41.444 and 2015 3rd sp.s. c 1 s 504 are each amended to read as follows:

(1) The shared information technology system revolving account is created in the custody of the state treasurer. All receipts from fees, charges for services, and assessments to agencies for shared information technology systems must be deposited into the account.

(2) Only the director or the director's designee may authorize expenditures from the account. The account is subject to allotment procedures under chapter 43.88 RCW, but no appropriation is required for expenditure.

(3) The office may contract with the ((~~consolidated technology services agency~~)) office of cybersecurity and information oversight for the billing of fees, charges for services, and assessments to agencies, and for the development, maintenance, and operations of shared information technology systems.

(4) For the purposes of this section, "shared information technology system" means an information technology system that is available to, but not required for use by, agencies.

**Sec.**  RCW 43.70.054 and 2015 3rd sp.s. c 1 s 408 are each amended to read as follows:

(1) To promote the public interest consistent with chapter 267, Laws of 1995, the department of health, in cooperation with the director of the ((~~consolidated technology services agency established in RCW 43.105.025~~)) office of cybersecurity and information oversight established under section 1 of this act, shall develop health care data standards to be used by, and developed in collaboration with, consumers, purchasers, health carriers, providers, and state government as consistent with the intent of chapter 492, Laws of 1993 as amended by chapter 267, Laws of 1995, to promote the delivery of quality health services that improve health outcomes for state residents. The data standards shall include content, coding, confidentiality, and transmission standards for all health care data elements necessary to support the intent of this section, and to improve administrative efficiency and reduce cost. Purchasers, as allowed by federal law, health carriers, health facilities and providers as defined in chapter 48.43 RCW, and state government shall ((~~utilize~~)) use the data standards. The information and data elements shall be reported as the department of health directs by rule in accordance with data standards developed under this section.

(2) The health care data collected, maintained, and studied by the department under this section or any other entity: (a) Shall include a method of associating all information on health care costs and services with discrete cases; (b) shall not contain any means of determining the personal identity of any enrollee, provider, or facility; (c) shall only be available for retrieval in original or processed form to public and private requesters; (d) shall be available within a reasonable period of time after the date of request; and (e) shall give strong consideration to data standards that achieve national uniformity.

(3) The cost of retrieving data for state officials and agencies shall be funded through state general appropriation. The cost of retrieving data for individuals and organizations engaged in research or private use of data or studies shall be funded by a fee schedule developed by the department that reflects the direct cost of retrieving the data or study in the requested form.

(4) All persons subject to this section shall comply with departmental requirements established by rule in the acquisition of data, however, the department shall adopt no rule or effect no policy implementing the provisions of this section without an act of law.

(5) The department shall submit developed health care data standards to the appropriate committees of the legislature by December 31, 1995.

**Sec.**  RCW 43.88.092 and 2015 3rd sp.s. c 1 s 410 are each amended to read as follows:

(1) As part of the biennial budget process, the office of financial management shall collect from agencies, and agencies shall provide, information to produce reports, summaries, and budget detail sufficient to allow review, analysis, and documentation of all current and proposed expenditures for information technology by state agencies. Information technology budget detail must be included as part of the budget submittal documentation required pursuant to RCW 43.88.030.

(2) The office of financial management must collect, and present as part of the biennial budget documentation, information for all existing information technology projects as defined by technology services board policy. The office of financial management must work with the office of the state chief information officer to maximize the ability to draw this information from the information technology portfolio management data collected by the ((~~consolidated technology services agency~~)) office of cybersecurity. Connecting project information collected through the portfolio management process with financial data developed under subsection (1) of this section provides transparency regarding expenditure data for existing technology projects.

(3) The ((~~director of the consolidated technology services agency~~)) chief information security officer shall evaluate proposed information technology expenditures and establish priority ranking categories of the proposals. No more than one-third of the proposed expenditures shall be ranked in the highest priority category.

(4) The biennial budget documentation submitted by the office of financial management pursuant to RCW 43.88.030 must include an information technology plan and a technology budget for the state identifying current baseline funding for information technology, proposed and ongoing major information technology projects, and their associated costs. This plan and technology budget must be presented using a method similar to the capital budget, identifying project costs through stages of the project and across fiscal periods and biennia from project initiation to implementation. This information must be submitted electronically, in a format to be determined by the office of financial management and the legislative evaluation and accountability program committee.

(5) The office of financial management shall also institute a method of accounting for information technology-related expenditures, including creating common definitions for what constitutes an information technology investment.

(6) For the purposes of this section, "major information technology projects" includes projects that have a significant anticipated cost, complexity, or are of statewide significance, such as enterprise-level solutions, enterprise resource planning, and shared services initiatives.

**Sec.**  RCW 43.88.160 and 2015 3rd sp.s. c 1 s 303 and 2015 3rd sp.s. c 1 s 109 are each reenacted and amended to read as follows:

This section sets forth the major fiscal duties and responsibilities of officers and agencies of the executive branch. The regulations issued by the governor pursuant to this chapter shall provide for a comprehensive, orderly basis for fiscal management and control, including efficient accounting and reporting therefor, for the executive branch of the state government and may include, in addition, such requirements as will generally promote more efficient public management in the state.

(1) Governor; director of financial management. The governor, through the director of financial management, shall devise and supervise a modern and complete accounting system for each agency to the end that all revenues, expenditures, receipts, disbursements, resources, and obligations of the state shall be properly and systematically accounted for. The accounting system shall include the development of accurate, timely records and reports of all financial affairs of the state. The system shall also provide for central accounts in the office of financial management at the level of detail deemed necessary by the director to perform central financial management. The director of financial management shall adopt and periodically update an accounting procedures manual. Any agency maintaining its own accounting and reporting system shall comply with the updated accounting procedures manual and the rules of the director adopted under this chapter. An agency may receive a waiver from complying with this requirement if the waiver is approved by the director. Waivers expire at the end of the fiscal biennium for which they are granted. The director shall forward notice of waivers granted to the appropriate legislative fiscal committees. The director of financial management may require such financial, statistical, and other reports as the director deems necessary from all agencies covering any period.

(2) Except as provided in chapter 43.88C RCW, the director of financial management is responsible for quarterly reporting of primary operating budget drivers such as applicable workloads, caseload estimates, and appropriate unit cost data. These reports shall be transmitted to the legislative fiscal committees or by electronic means to the legislative evaluation and accountability program committee. Quarterly reports shall include actual monthly data and the variance between actual and estimated data to date. The reports shall also include estimates of these items for the remainder of the budget period.

(3) The director of financial management shall report at least annually to the appropriate legislative committees regarding the status of all appropriated capital projects, including transportation projects, showing significant cost overruns or underruns. If funds are shifted from one project to another, the office of financial management shall also reflect this in the annual variance report. Once a project is complete, the report shall provide a final summary showing estimated start and completion dates of each project phase compared to actual dates, estimated costs of each project phase compared to actual costs, and whether or not there are any outstanding liabilities or unsettled claims at the time of completion.

(4) In addition, the director of financial management, as agent of the governor, shall:

(a) Develop and maintain a system of internal controls and internal audits comprising methods and procedures to be adopted by each agency that will safeguard its assets, check the accuracy and reliability of its accounting data, promote operational efficiency, and encourage adherence to prescribed managerial policies for accounting and financial controls. The system developed by the director shall include criteria for determining the scope and comprehensiveness of internal controls required by classes of agencies, depending on the level of resources at risk.

(i) For those agencies that the director determines internal audit is required, the agency head or authorized designee shall be assigned the responsibility and authority for establishing and maintaining internal audits following professional audit standards including generally accepted government auditing standards or standards adopted by the institute of internal auditors, or both.

(ii) For those agencies that the director determines internal audit is not required, the agency head or authorized designee may establish and maintain internal audits following professional audit standards including generally accepted government auditing standards or standards adopted by the institute of internal auditors, or both, but at a minimum must comply with policies as established by the director to assess the effectiveness of the agency's systems of internal controls and risk management processes;

(b) Make surveys and analyses of agencies with the object of determining better methods and increased effectiveness in the use of manpower and materials; and the director shall authorize expenditures for employee training to the end that the state may benefit from training facilities made available to state employees;

(c) Establish policies for allowing the contracting of child care services;

(d) Report to the governor with regard to duplication of effort or lack of coordination among agencies;

(e) Review any pay and classification plans, and changes thereunder, developed by any agency for their fiscal impact: PROVIDED, That none of the provisions of this subsection shall affect merit systems of personnel management now existing or hereafter established by statute relating to the fixing of qualifications requirements for recruitment, appointment, or promotion of employees of any agency. The director shall advise and confer with agencies including appropriate standing committees of the legislature as may be designated by the speaker of the house and the president of the senate regarding the fiscal impact of such plans and may amend or alter the plans, except that for the following agencies no amendment or alteration of the plans may be made without the approval of the agency concerned: Agencies headed by elective officials;

(f) Fix the number and classes of positions or authorized employee years of employment for each agency and during the fiscal period amend the determinations previously fixed by the director except that the director shall not be empowered to fix the number or the classes for the following: Agencies headed by elective officials;

(g) Adopt rules to effectuate provisions contained in (a) through (f) of this subsection.

(5) The treasurer shall:

(a) Receive, keep, and disburse all public funds of the state not expressly required by law to be received, kept, and disbursed by some other persons: PROVIDED, That this subsection shall not apply to those public funds of the institutions of higher learning which are not subject to appropriation;

(b) Receive, disburse, or transfer public funds under the treasurer's supervision or custody;

(c) Keep a correct and current account of all moneys received and disbursed by the treasurer, classified by fund or account;

(d) Coordinate agencies' acceptance and use of credit cards and other payment methods, if the agencies have received authorization under RCW 43.41.180;

(e) Perform such other duties as may be required by law or by regulations issued pursuant to this law.

It shall be unlawful for the treasurer to disburse public funds in the treasury except upon forms or by alternative means duly prescribed by the director of financial management. These forms or alternative means shall provide for authentication and certification by the agency head or the agency head's designee that the services have been rendered or the materials have been furnished; or, in the case of loans or grants, that the loans or grants are authorized by law; or, in the case of payments for periodic maintenance services to be performed on state owned equipment, that a written contract for such periodic maintenance services is currently in effect; and the treasurer shall not be liable under the treasurer's surety bond for erroneous or improper payments so made. When services are lawfully paid for in advance of full performance by any private individual or business entity other than equipment maintenance providers or as provided for by RCW 42.24.035, such individual or entity other than central stores rendering such services shall make a cash deposit or furnish surety bond coverage to the state as shall be fixed in an amount by law, or if not fixed by law, then in such amounts as shall be fixed by the director of the department of enterprise services but in no case shall such required cash deposit or surety bond be less than an amount which will fully indemnify the state against any and all losses on account of breach of promise to fully perform such services. No payments shall be made in advance for any equipment maintenance services to be performed more than twelve months after such payment except that institutions of higher education as defined in RCW 28B.10.016 and the ((~~consolidated technology services agency created in RCW 43.105.006~~)) office of cybersecurity and information oversight established under section 1 of this act may make payments in advance for equipment maintenance services to be performed up to sixty months after such payment. Any such bond so furnished shall be conditioned that the person, firm or corporation receiving the advance payment will apply it toward performance of the contract. The responsibility for recovery of erroneous or improper payments made under this section shall lie with the agency head or the agency head's designee in accordance with rules issued pursuant to this chapter. Nothing in this section shall be construed to permit a public body to advance funds to a private service provider pursuant to a grant or loan before services have been rendered or material furnished.

(6) The state auditor shall:

(a) Report to the legislature the results of current post audits that have been made of the financial transactions of each agency; to this end the auditor may, in the auditor's discretion, examine the books and accounts of any agency, official, or employee charged with the receipt, custody, or safekeeping of public funds. Where feasible in conducting examinations, the auditor shall utilize data and findings from the internal control system prescribed by the office of financial management. The current post audit of each agency may include a section on recommendations to the legislature as provided in (c) of this subsection.

(b) Give information to the legislature, whenever required, upon any subject relating to the financial affairs of the state.

(c) Make the auditor's official report on or before the thirty-first of December which precedes the meeting of the legislature. The report shall be for the last complete fiscal period and shall include determinations as to whether agencies, in making expenditures, complied with the laws of this state. The state auditor is authorized to perform or participate in performance verifications and performance audits as expressly authorized by the legislature in the omnibus biennial appropriations acts or in the performance audit work plan approved by the joint legislative audit and review committee. The state auditor, upon completing an audit for legal and financial compliance under chapter 43.09 RCW or a performance verification, may report to the joint legislative audit and review committee or other appropriate committees of the legislature, in a manner prescribed by the joint legislative audit and review committee, on facts relating to the management or performance of governmental programs where such facts are discovered incidental to the legal and financial audit or performance verification. The auditor may make such a report to a legislative committee only if the auditor has determined that the agency has been given an opportunity and has failed to resolve the management or performance issues raised by the auditor. If the auditor makes a report to a legislative committee, the agency may submit to the committee a response to the report. This subsection (6) shall not be construed to authorize the auditor to allocate other than de minimis resources to performance audits except as expressly authorized in the appropriations acts or in the performance audit work plan. The results of a performance audit conducted by the state auditor that has been requested by the joint legislative audit and review committee must only be transmitted to the joint legislative audit and review committee.

(d) Be empowered to take exception to specific expenditures that have been incurred by any agency or to take exception to other practices related in any way to the agency's financial transactions and to cause such exceptions to be made a matter of public record, including disclosure to the agency concerned and to the director of financial management. It shall be the duty of the director of financial management to cause corrective action to be taken within six months, such action to include, as appropriate, the withholding of funds as provided in RCW 43.88.110. The director of financial management shall annually report by December 31st the status of audit resolution to the appropriate committees of the legislature, the state auditor, and the attorney general. The director of financial management shall include in the audit resolution report actions taken as a result of an audit including, but not limited to, types of personnel actions, costs and types of litigation, and value of recouped goods or services.

(e) Promptly report any irregularities to the attorney general.

(f) Investigate improper governmental activity under chapter 42.40 RCW.

In addition to the authority given to the state auditor in this subsection (6), the state auditor is authorized to conduct performance audits identified in RCW 43.09.470. Nothing in this subsection (6) shall limit, impede, or restrict the state auditor from conducting performance audits identified in RCW 43.09.470.

(7) The joint legislative audit and review committee may:

(a) Make post audits of the financial transactions of any agency and management surveys and program reviews as provided for in chapter 44.28 RCW as well as performance audits and program evaluations. To this end the joint committee may in its discretion examine the books, accounts, and other records of any agency, official, or employee.

(b) Give information to the legislature or any legislative committee whenever required upon any subject relating to the performance and management of state agencies.

(c) Make a report to the legislature which shall include at least the following:

(i) Determinations as to the extent to which agencies in making expenditures have complied with the will of the legislature and in this connection, may take exception to specific expenditures or financial practices of any agencies; and

(ii) Such plans as it deems expedient for the support of the state's credit, for lessening expenditures, for promoting frugality and economy in agency affairs, and generally for an improved level of fiscal management.

**Sec.**  RCW 44.68.065 and 2020 c 114 s 13 are each amended to read as follows:

The legislative service center, under the direction of the joint legislative systems administrative committee, shall:

(1) Develop a legislative information technology portfolio consistent with the provisions of RCW 43.105.341;

(2) Participate in the development of an enterprise-based statewide information technology strategy;

(3) Ensure the legislative information technology portfolio is organized and structured to clearly indicate participation in and use of enterprise-wide information technology strategies;

(4) As part of the biennial budget process, submit the legislative information technology portfolio to the chair and ranking member of the ways and means committees of the house of representatives and the senate, the office of financial management, and the ((~~consolidated technology services agency~~)) office of cybersecurity and information oversight.

**Sec.**  RCW 46.20.157 and 2011 1st sp.s. c 43 s 811 are each amended to read as follows:

(1) Except as provided in subsection (2) of this section, the department shall annually provide to the ((~~consolidated technology services agency~~)) office of cybersecurity and information oversight an electronic data file. The data file must:

(a) Contain information on all licensed drivers and identicard holders who are eighteen years of age or older and whose records have not expired for more than two years;

(b) Be provided at no charge; and

(c) Contain the following information on each such person: Full name, date of birth, residence address including county, sex, and most recent date of application, renewal, replacement, or change of driver's license or identicard.

(2) Before complying with subsection (1) of this section, the department shall remove from the file the names of any certified participants in the Washington state address confidentiality program under chapter 40.24 RCW that have been identified to the department by the secretary of state.

**Sec.**  RCW 50A.25.070 and 2020 c 125 s 8 are each amended to read as follows:

(1) The department may enter into data-sharing contracts and may disclose records and information deemed confidential to state or local government agencies under this chapter only if permitted under subsection (2) of this section and RCW 50A.25.090. A state or local government agency must need the records or information for an official purpose and must also provide:

(a) An application in writing to the department for the records or information containing a statement of the official purposes for which the state or local government agency needs the information or records and specifically identify the records or information sought from the department; and

(b) A written verification of the need for the specific information from the director, commissioner, chief executive, or other official of the requesting state or local government agency either on the application or on a separate document.

(2) The department may disclose information or records deemed confidential under this chapter to the following state or local government agencies:

(a) To the department of social and health services to identify child support obligations as defined in RCW 50A.15.080;

(b) To the department of revenue to determine potential tax liability or employer compliance with registration and licensing requirements;

(c) To the department of labor and industries to compare records or information to detect improper or fraudulent claims;

(d) To the office of financial management for the purpose of conducting periodic salary or fringe benefit studies pursuant to law;

(e) To the office of the state treasurer and any financial or banking institutions deemed necessary by the office of the state treasurer and the department for the proper administration of funds;

(f) To the office of the attorney general for purposes of legal representation;

(g) To a county clerk for the purpose of RCW 9.94A.760 if requested by the county clerk's office;

(h) To the office of administrative hearings for the purpose of administering the administrative appeal process;

(i) To the department of enterprise services for the purpose of agency administration and operations; and

(j) To the ((~~consolidated technology services agency~~)) office of cybersecurity and information oversight for the purpose of enterprise technology support.

**Sec.**  RCW 2.68.060 and 2015 3rd sp.s. c 1 s 403 are each amended to read as follows:

The administrative office of the courts, under the direction of the judicial information system committee, shall:

(1) Develop a judicial information system information technology portfolio consistent with the provisions of RCW 43.105.341;

(2) Participate in the development of an enterprise-based statewide information technology strategy;

(3) Ensure the judicial information system information technology portfolio is organized and structured to clearly indicate participation in and use of enterprise-wide information technology strategies;

(4) As part of the biennial budget process, submit the judicial information system information technology portfolio to the chair and ranking member of the ways and means committees of the house of representatives and the senate, the office of financial management, and the ((~~consolidated technology services agency~~)) office of cybersecurity.

NEW SECTION. **Sec.**  The following acts or parts of acts are each repealed:

(1)RCW 43.105.006 (Consolidated technology services agency—Purpose) and 2011 1st sp.s. c 43 s 801; and

(2)RCW 43.105.215 (Security standards and policies—State agencies' information technology security programs) and 2015 3rd sp.s. c 1 s 202 & 2013 2nd sp.s. c 33 s 8."

Correct the title.

EFFECT: **(1) Restructuring and the Office of Cybersecurity generally:**

(a) Restructures the Consolidated Technology Services Agency (WaTech) so that the Office of Cybersecurity and Information Oversight (OCS) is as an agency of state government and WaTech is an office within the OCS; and makes conforming changes throughout the striking amendment.

(b) Requires the Governor, rather than the Chief Information Officer who is the Director of WaTech (Director), to appoint the State Chief Information Security Officer (CISO) who is the director of the OCS and determine the CISO's salary.

(c) Adds as a duty of the CISO the duty to act as a central manager of the state information technology (IT) infrastructure and programs, and to oversee the functions of the OCS and the officers established within the OCS.

(d) Requires that the OCS, by January 15th each year, submit a report to the Legislature that details the efficacy and cost-effectiveness of the state's efforts to protect the state's IT systems and infrastructure from cybersecurity threats and attacks.

(e) Requires the OCS to establish rates and fees for services included the catalog of cybersecurity services published by the OCS.

**(2) Transfers or modifications of existing statutory duties and powers of WaTech or its Director:**

(a) Transfers, from the Director to the CISO, the authority to:

(i) Create such administrative structures as appropriate;

(ii) Delegate powers/duty vested in him/her; and

(iii) Appoint a confidential secretary and employees to administer the agency.

(b) Makes the authority of the Director to accept and spend gifts and grants and to apply for grants subject to the approval of the CISO.

(c) Modifies the Director's authority to establish rates and fees for services provided by WaTech to remove the authority to set rates and fees related to the catalog of cybersecurity services published by the OCS.

(d) Transfers the requirement to establish standards and policies to govern IT in the state from the Director to the CISO.

(e) Modifies the Office of the Chief Information Officer's (OCIO) authority to establish policies for the periodic review of the Director of cybersecurity to require that the establishment of the policies occur in coordination with the CISO.

(f) Transfers the requirement to adopt rules from WaTech to the OCS.

(g) Transfers the requirement to set performance targets and approve plans for achieving measurable and specific goals for the agency, from the Director to the CISO.

(h) Transfers the responsibility to develop, publish, and update a dashboard of key performance measures. Requires the OCS, rather than WaTech, develop the dashboard that is published on OCS's website.

(i) Transfers the responsibility to report quarterly to the Governor on the agency's performance from the Director to the CISO.

(j) Requires the CISO, rather than the Director, to use agency IT portfolio planning to develop a statewide portfolio that guides resource allocation and prioritization decisions.

(k) Authorizes the CISO, rather than the Director, to exempt a state agency from any or all requirements to develop an agency IT portfolio.

(l) Authorizes the CISO, rather than the Director, to suspend or terminate a major IT project for specified reasons.

(m) Authorizes the CISO, rather than the Director, to require a state agency to procure a product or service through the OCS, rather than WaTech, if a substantially similar product or service is offered by the OCS.

(n) Requires the OCS, rather than WaTech, to periodically review major IT systems used by state agencies.

(o) Requires the CISO, rather than the Director, to appoint the Chief Privacy Officer of the Office of Privacy and Data Protection.

(p) Requires the CISO, rather than the Director, to evaluate proposed IT expenditures as part of the biennial budget process and establish priority ranking categories of the proposals.

**(3) Other modifications to existing statutes, primarily pertaining to state agency interactions with WaTech:**

(a) Authorizes state and local governments to enter contracts with the OCS, rather than WaTech.

(b) Requires that the advice of the CISO, rather than the Director, be sought by OFM when OFM requires incremental funding of a project on a phase-by-phase basis where the previous phase is satisfactorily completed.

(c) Authorizes the Technology Services Board (TSB) to review and approve standards and policies developed by the OCS governing the protection and oversight of the state's IT systems and infrastructure, and cybersecurity prevention and response protocols.

(d) Exempts the OCS, rather than WaTech, from requirements of contracting out for services under the civil service statute, if certain conditions are met.

(e) Renames the Consolidated Technology Services Revolving Account the Office of Cybersecurity and Information Oversight Revolving Account; authorizes only the CISO, rather than the Director, to approve expenditures from the account; and makes other conforming changes.

(f) Requires that the migration strategy established under current law by the Office of the Chief Information Officer (OCIO) be a migration strategy to move towards using the OCS, rather than WaTech, as the central services provider for all utility-based infrastructure services used by state agencies.

(g) Makes conforming changes to current law relating to affirming that the agency does not have any additional authority over providers of telecommunications and IT.

(h) Clarifies that provisions in the section transferring powers, duties, and functions of the former Department of Information Services (DIS) to WaTech remain unless otherwise specified by this act.

(i) Changes references to WaTech in current procurement statutes to the OCS, where the statute exempts WaTech from existing procurement laws if certain conditions are met.

(j) Modifies current law that specifies that the procurement laws do not pertain to IT purchases by state agencies under certain conditions, including if the initial purchase is approved by the Director to instead state that procurement laws do not pertain to IT purchases if the initial purchase is approved by the CISO.

(k) Makes conforming changes to civil service laws to specify that certain employees of OCS (rather than WaTech) are exempt from civil service.

(l) Makes conforming changes to civil service laws to specify that up to 12 positions in policy development or senior professionals of OCS (rather than WaTech) are exempt from civil service.

(m) Makes conforming changes to the campaign finance statute and specifies that the definition of "executive state officer" as used in the campaign finance statute includes the CISO rather than the Director.

(n) Requires that the Office of Financial Management's (OFM) coordinated budget for network development, operation, and expansion include the CISO's, rather than the Director's, recommendations on certain elements.

(o) Authorizes the OFM to contract with the OCS, rather than WaTech, for the billing of fees, charges for services, and assessments to agencies, and for the maintenance and operations of enterprise IT systems, in relation to the Statewide IT System Maintenance and Operations Revolving Account.

(p) Authorizes OFM to contract with the OCS, rather than WaTech, for the billing of fees, charges for services, and assessments to agencies, and for the development, maintenance, and operations of shared IT systems, in relation to the Shared IT System Revolving Account.

(q) Modifies the requirement that the Department of Health (DOH) cooperate with the Director when developing health care data standards to instead require DOH to cooperate with the CISO.

(r) Changes references of the agency that collects state agency IT portfolio management data from WaTech to OCS.

(s) Changes conforming changes to name the OCS, rather than WaTech, in current statute reflecting major fiscal duties and responsibilities of officers and agencies of the executive branch.

(t) Requires that the Legislative Service Center, as part of the biennial budget process, submit its IT portfolio to the OCS, rather than WaTech.

(u) Requires that the Department of Licensing submit to the OCS, rather than WaTech, an electronic file annually of information on all licensed drivers and identicard holders who are 18 years of age or older.

(v) Authorizes the Employment Security Department to enter into data-sharing contracts and disclose confidential records and information to the OCS, rather than WaTech.

(w) Requires that the Administrative Office of the Courts, as part of the biennial budget process, submit its IT portfolio to the OCS, rather than WaTech.