AMENDMENTS TO HOUSE BILL NO. 40

Sponsor: REPRESENTATIVE RYAN

Printer's No. 19

Amend Bill, page 1, lines 1 through 7, by striking out all of said lines and inserting

Amending Title 71 (State Government) of the Pennsylvania Consolidated Statutes, in boards and offices, providing for information technology; establishing the Office of Information Technology and the Information Technology Fund; providing for administrative and procurement procedures and for the Joint Cybersecurity Oversight Committee; imposing duties on the Office of Information Technology; providing for administration of Pennsylvania Statewide Radio Network and imposing penalties.

Amend Bill, page 1, lines 10 through 20; pages 2 through 45, lines 1 through 30; page 46, lines 1 through 15; by striking out all of said lines on said pages and inserting

Section 1. Part V of Title 71 of the Pennsylvania Consolidated Statutes is amended by adding a chapter to read:

CHAPTER 43

INFORMATION TECHNOLOGY

Subchapter

A. General Provisions

B. Office of Information Technology

C. Business Operations

D. Procurement of Information Technology

E. Security

F. Enforcement and Penalties

G. Pennsylvania Statewide Radio Network

SUBCHAPTER A

GENERAL PROVISIONS

Sec.

4301. Scope of chapter.

4302. Findings and declarations.

4303. Definitions.

§ 4301. Scope of chapter.

This chapter relates to administrative procedures and procurement regarding information technology.

§ 4302. Findings and declarations.

The General Assembly finds and declares the following:

(1) The Commonwealth has struggled to keep information technology costs under control, including failing to include as part of overall costs, time spent by Commonwealth staff for development, implementation and use of information technology.

(2) Many of the Commonwealth's information technology contracts extend well beyond their anticipated date of completion.

(3) The Commonwealth can begin to reduce information technology costs by the consolidation of information technology functions and resources within the executive branch.

(4) Consolidation of information technology services will not only reduce costs but create more efficient information technology operations.

(5) By reforming the Commonwealth's outdated approach to information technology, the Commonwealth can improve data and analytic capabilities and improve cybersecurity.

(6) The improvement of operations will enhance taxpayer satisfaction and make it easier for residents to navigate.

(7) Consolidation of information technology services must be designed to improve accountability and transparency to taxpayers and enhance the Commonwealth's data and analytics capabilities.

(8) The Commonwealth shall, as part of its information technology and cybersecurity efforts:

(i) Reduce redundancy and align information technology spending in a manner that reduces costs and measurably improves Commonwealth agency mission effectiveness.

(ii) Improve quality, transparency and accountability in the procurement and use of information technology.

(iii) Achieve five-year budget limits, within limited variance, for all administrative agencies for projects above a de minimis threshold.

(iv) Achieve measurable protection for Commonwealth data, including identifying and mitigating risks for personal identifiable information and other valuable, nonpublic mission critical data.

§ 4303. Definitions.

The following words and phrases when used in this chapter shall have the meanings given to them in this section unless the context clearly indicates otherwise:

"Architecture." The overall design of a computing system and the logical and physical interrelationships between its components.

"Authorization to operate." A formal declaration by the head of the State agency that:

(1) authorizes operation of a product and explicitly accepts the risk to agency operations; and

(2) is signed after the system has met and passed all requirements to become operational.

"Business case." A statement specifying the needs of the State agency for information technology, services and related resources, including expected improvements to programmatic or business operations, and the requirements for State resources and funding, together with an evaluation of those requirements by the chief information officer assigned to the State agency which takes into consideration:

(1) The State's current technology.

(2) The opportunities for technology sharing.

(3) Any other factors relevant to the analysis by the director.

"Director." The administrative head of the office and chief information officer of the Commonwealth.

"Distributed information technology assets." Hardware, software and communications equipment not classified as traditional mainframe-based items, including, but not limited to, personal computers, local area networks, servers, mobile computers, peripheral equipment and other related hardware and software items.

"Electronic bidding." The electronic solicitation and receipt of offers to contract.

"Fund." The Information Technology Fund established under section 4316 (relating to Commonwealth Information Technology Fund).

"Independent agency." As follows:

(1) A board, commission, authority or other agency of the Commonwealth that is not subject to the policy supervision and control of the Governor.

(2) The term does not include:

(i) A court or agency of the unified judicial system.

(ii) The General Assembly or an agency of the General Assembly.

"Independent department." Any of the following:

(1) The Department of the Auditor General.

(2) The Treasury Department.

(3) The Office of Attorney General.

(4) A board or commission of an entity under paragraph (1), (2) or (3).

"Information technology." Hardware, software and telecommunications equipment, including, but not limited to, the following:

(1) Personal computers.

(2) Servers.

(3) Mainframes.

(4) Wired or wireless wide and local area networks.

(5) Broadband.

(6) Mobile or portable computers.
(7) Peripheral equipment.
(8) Telephones.
(9) Wireless communications.
(10) Handheld devices.
(11) Facsimile machines.
(12) Technology facilities, including, but not limited to, data centers, dedicated training facilities or switching facilities.
(13) Electronic payment processing services.
(14) Other relevant hardware and software items or personnel tasked with the planning, implementation or support of technology, including hosting or vendor-managed service solutions.

"Information technology budget." As follows:

(1) All information technology expenditures listed by project and amount of expenditure for planning, development, modernization, operations and maintenance.
(2) The term includes all software, hardware, Commonwealth and vendor staff and service costs.

"Information technology security incident." A computer-based activity, network-based activity or paper-based activity that results directly or indirectly in misuse, damage, denial of service, compromise of integrity or loss of confidentiality of a network, a computer, an application or data.

"Office." The Office of Information Technology established under Subchapter B (relating to Office of Information Technology).

"Open data." Government data sets and documents that are considered publicly available under the act of February 14, 2008 (P.L.6, No.3), known as the Right-to-Know Law, or other Commonwealth transparency initiatives to use and republish without restriction from copyright, patents or other restrictions on control.

"Portal." A publicly available Internet website.

"Reverse auction." A real-time purchasing process in which vendors compete to provide goods or services at the lowest selling price in an open and interactive electronic environment.

"Secretary." The Secretary of Administration of the Commonwealth.

"State agency." Any of the following:

(1) The Governor's Office.
(2) A department, board, commission, authority or other agency of the Commonwealth that is subject to the policy supervision and control of the Governor.
(3) The office of Lieutenant Governor.
(4) An independent agency.

SUBCHAPTER B
OFFICE OF INFORMATION TECHNOLOGY

Sec.
4311. Establishment of office.

§ 4311. Establishment of office.

The Office of Information Technology is established within the Governor's Office of Administration to oversee and achieve information technology consolidation and other findings of this chapter.

§ 4312. Duties of office.

(a) Duties generally.--The office shall:

(1) Consolidate information technology functions, powers, duties, obligations, infrastructure and support services vested in State agencies.

(2) Provide, operate and manage the information technology services for each State agency under the Governor's jurisdiction, including, but not limited to, the following:

(i) The development of priorities and strategic plans.

(ii) The management of information technology investments, procurement and policy.

(iii) Compliance with the provisions of this chapter through consultation and engagement with the secretary of each agency.

(3) Notwithstanding any other provisions of law, procure all information technology and information technology as a service for State agencies utilizing the processes under 62 Pa.C.S. Ch. 5 (relating to source selection and contract formation). The office shall integrate technological review, cost analysis and procurement for all information technology needs of State agencies to make procurement and implementation of technology more responsive, efficient and cost effective.

(4) Determine any changes to staffing or operations regarding information technology.

(5) Provide documentation and training to achieve development in the functional responsibilities that shall include:

(i) Defining an information technology strategy plan.

(ii) Defining enterprise architecture.

(iii) Determining technological direction.

(iv) Defining information technology organization and relationships.

(v) Managing information technology investment.

(vi) Communicating management aims and direction.

(vii) Managing information technology human resources.

(viii) Managing quality.

(ix) Assessing risks.

(x) Managing projects.

(xi) Identifying automated solutions.

(xii) Acquiring and maintaining application software.

(xiii) Acquiring and maintaining technology infrastructure.

(xiv) Enabling operation and use.

(xv) Procuring information technology resources.

(xvi) Managing changes.

(xvii) Installing and accrediting solutions and changes.

(xviii) Defining and managing service levels.

(xix) Managing third-party services.

(xx) Managing performance and capacity.

(xxi) Ensuring continuous service.

(xxii) Ensuring system security.

(xxiii) Identifying and allocating costs.

(xxiv) Educating and training users.

(xxv) Managing service desk and incidents.

(xxvi) Managing the configuration.

(xxvii) Managing problems.

(xxviii) Managing data.

(xxix) Managing physical environment.

(xxx) Managing operations.

(xxxi) Monitoring and evaluating information technology performance.

(xxxii) Monitoring and evaluating internal controls.

(xxxiii) Ensuring compliance with external requirements.

(xxxiv) Providing improved information technology governance.

(b) Specific duties.--As part of the general duties under subsection (a), the office shall:

(1) Develop and administer a comprehensive long-range plan to ensure the proper management of the information technology resources of the Commonwealth.

(2) Set technical standards for information technology and review and approve information technology projects and budgets.

(3) Establish information technology security standards.

(4) Provide for the procurement of information technology resources.

(5) Develop a schedule for the replacement or

modification of information technology systems.

(6) Prescribe the manner in which information technology assets, systems and personnel shall be provided and distributed among State agencies.

(7) Prescribe the manner of inspecting or testing information technology assets, systems or personnel to determine compliance with information technology plans, specifications and requirements.

(8) Develop an annual information technology strategic plan that aligns information technology expenditures with each State agency's strategic initiatives and ongoing mission needs, including priorities resource use and expenditures, performance review measures, procurement and other governance and planning measures.

(9) Provide guidance, review and approve the information technology plans for each State agency.

(10) Obtain guidance and consult with the Office of the Budget on budgetary matters regarding information technology spending and procurement plans.

(11) Obtain advice on matters involving overall technology and data governance from academia, private sector and other leading government institutions.

(12) Establish and maintain an information technology portfolio management process to prepare and manage the information technology budget, including overall monitoring of information technology program objectives and alignment with administrative priorities, budgets and expenditures.

(13) Identify common information technology business functions within each State agency.

(14) Make recommendations for consolidation, integration and investment.

(15) Facilitate the use of common technology, as appropriate.

(16) Ensure the proper use of project management methodologies and principles on information technology projects, including measures to review project delivery and quality.

(17) Ensure compliance by each State agency with required business process reviews.

(18) Audit the information technology assets of each State agency no later than 547 days after the effective date of this paragraph.

(19) Serve as a liaison between State agencies and contracted information technology vendors.

(20) Align the appropriate technology and procurement methods with the service strategy.

(21) Establish and maintain an information technology architecture that ensures a modern operating environment for agencies and aligns all information technology investments to the information technology strategic plan. This architecture shall include the following, as appropriate:

(i) The development of standards, policies, processes and strategic technology roadmaps.

(ii) The performance of technical reviews and capability assessments of services, technologies and State agency systems.

(iii) The evaluation of requests for information technology policy exceptions.

(iv) The ability to incorporate emerging technologies in a cost-effective and timely manner.

(22) Develop and implement efforts to standardize data elements and determine data ownership assignments.

(23) Establish and operate centers of expertise for specific information technologies and services to serve two or more State agencies on a cost-sharing basis, if the director, after consultation with the Office of the Budget, decides it is advisable from the standpoint of the information technology strategic plan, efficiency and economy to establish these centers and services.

(24) Require a State agency served to transfer to the office ownership, custody or control of information processing equipment, supplies and positions required to implement the information technology strategic plan.

(25) Develop and promote training programs to efficiently implement, use and manage information technology resources throughout State government.

(26) Develop and maintain a comprehensive information technology inventory.

(27) Monitor compliance with information technology policy and standards through investment, budgeting and architectural review processes.

(28) Maintain and strengthen the Commonwealth's cybersecurity posture through security governance.

(29) Develop security solutions, services and programs to protect data and infrastructure.

(30) Identify and remediate security risks and maintain citizen trust in securing computerized personal information.

(31) Implement programs, processes and solutions to maintain cybersecurity situational awareness and effectively respond to cybersecurity attacks and information technology security incidents.

(32) Create a process identifying risks to the success of information technology programs and projects, developing mitigations, incorporating mitigating actions in budgeting and investment and review processes.

(33) Conduct evaluations and compliance audits of State agency security infrastructure.

(34) Develop and produce cost, risk and quality initiatives that consolidate State agency information technology services, including, but not limited to, infrastructure, personnel, investments, operations and support services necessary to achieve the findings of this

chapter.

(35) Establish and facilitate a process for the identification, evaluation and optimization of information technology shared services.

(36) Establish a process for the following:

(i) Developing and implementing telecommunications policies, services and infrastructure.

(ii) Reviewing and authorizing State agency requests for enhanced services.

(37) Identify opportunities for convergence and leveraging existing assets to reduce or eliminate duplicative telecommunication networks.

(38) Establish, maintain and continuously optimize cost and performance of an information technology service management process library and services catalog to govern the services provided to each State agency.

(39) Establish a formal operational testing environment to enable the rapid evaluation and introduction of new information technology services and the retiring of existing information technology services.

(40) Establish metrics to monitor the health of the services provided and make appropriate corrections as necessary.

(41) Establish information technology data management and development policy frameworks throughout each State agency that include policies, processes and standards that adhere to commonly accepted principles for, among other things, data governance, data development and the quality, sourcing, use, accessibility, content, ownership and licensing of open data.

(42) Create and maintain a comprehensive open data portal for public accessibility.

(43) Provide guidance regarding the procurement of supplies and services related to the subject matter of this chapter.

(44) Facilitate communication with the public by publishing open data plans and policies and by soliciting or allowing for public input on the subject matter of this chapter.

(45) Ensure the internal examination of Commonwealth data sets for business, confidentiality, privacy and security issues and the reasonable mitigation of those issues, prior to the data's release for open data purposes.

(46) Develop and facilitate the engagement with private and other public stakeholders, including, but not limited to, arranging for and expediting data-sharing agreements and encouraging and facilitating cooperation and substantive and administrative efficiencies.

(47) Develop and facilitate data sharing and data analytics to minimize redundancy and align information technology spending in a manner that reduces costs and

measurably improves Commonwealth agency mission effectiveness.

(48) Oversee the information technology contracts of each State agency. The following shall apply:

(i) The office shall obtain, review and maintain, on an ongoing basis, records of the appropriations, allotments, expenditures and revenues of each State agency for information technology.

(ii) The office shall identify opportunities for consolidation of redundant expenditures that could be more cost effectively provided through multiagency shared services.

(iii) The office shall conduct annual reviews of agency programs and contract cost estimates to ensure accuracy and quality in budgetary estimates.

(c) Discretionary duties.--Notwithstanding any other provision of law, the office may provide information technology services on a cost-sharing basis to the following:

(1) An independent department as requested by the head of the independent department.

(2) The General Assembly and its agencies as requested by the President pro tempore of the Senate and the Speaker of the House of Representatives.

(3) The judicial branch as requested by the Chief Justice of Pennsylvania.

§ 4313. Director.

(a) Appointment and salary.--The secretary shall appoint the director and set the starting salary of the director.

(b) Qualifications.--The director must be qualified by experience for the office and have at least five years of experience dealing with public sector information systems in a State government agency or an equivalent entity. The qualifications shall include, but are not limited to, verifying that an individual has the proper industry certifications necessary to perform the duties under this chapter.

(c) Duties.--In addition to other duties specified under this chapter, the director shall:

(1) Manage the operations of the office in a manner conducive to achieving the findings of this chapter.

(2) Review and approve reports by each State agency concerning information technology assets, systems, personnel and projects and prescribe the form of the reports.

(3) Hire personnel as necessary to perform the functions of the office.

(4) Provide written determination to the Secretary of the Budget of findings, remediation plan and restructuring actions for programs designated as the color red in accordance with section 4319 (relating to Statewide information technology transparency portal).

(5) Notify the Treasury Department in order to suspend funding for a program that has been designated as the color

red in accordance with section 4321 (relating to status of information technology projects and corrective action plans).

(d) Oversight.--The director shall oversee the manner and means by which information technology business and disaster recovery plans for State agencies are created, reviewed and updated.

(e) Disaster recovery plan.--

(1) The director shall ensure that each State agency establish a disaster recovery planning team and work with the office to develop a disaster recovery plan and administer and implement the plan.

(2) In developing a disaster recovery plan, all of the following shall be completed:

(i) Consideration of the organizational, managerial and technical environments in which the plan must be implemented.

(ii) An assessment of the types and likely parameters of disasters most likely to occur and the resultant impacts on the State agency's ability to perform its mission.

(iii) The listing of the protective measures to be implemented in anticipation of a natural or manmade disaster.

(iv) A determination whether the plan is adequate to address information technology security incidents.

(3) Each State agency shall submit its disaster recovery plan to the director on an annual basis and as otherwise requested by the director.

§ 4314. Transfer of additional duties and personnel.

Upon the effective date of this section, information technology functions, powers, duties, obligations and services shall be transferred to and organized to the maximum extent practicable into centers that provide shared services to State agencies. The following shall apply:

(1) The chief information officer of each State agency or shared service center shall:

(i) Report directly to the director.

(ii) Work within the chief information officer's respective State agency or shared service center on behalf of the office as an employee of the office.

(2) An employee of a State agency who handles or otherwise has responsibility for the State agency's information technology services shall be transferred to the office and operate in the physical location of the State agency or the shared services center supporting that agency, but the employee shall report matters to the office and be supervised by the chief information officer of the State agency or head of the shared services center.

(3) The chief information officer of each agency or shared service center shall be responsible for identifying and implementing actions and milestones as required to

fulfill the remediation plan determined by the director under section 4313(c)(4) (relating to director).

(4) Each State agency shall provide personnel if necessary to participate in project management, implementation, testing, shared services and other activities for an information technology project.

§ 4315. Planning and financing information technology resources.

(a) Development of policies.--The director shall issue necessary policies for State agency information technology planning and financing consistent with the findings under section 4302 (relating to findings and declarations).

(b) Development of plan.--

(1) The director shall analyze the needs for information and information technology systems and develop a plan to ascertain the needs, costs and time frame required for State agencies to efficiently use information technology systems, resources, security and data management to achieve the purposes of this chapter. The following shall apply:

(i) The plan may include current applications and infrastructure, migration from current environments and other information necessary for fiscal or technology planning.

(ii) The plan shall include a budget for all information technology expenditures.

(2) In consultation with the Secretary of the Budget, the office shall develop and implement a plan to manage all information technology funding, including Commonwealth and other receipts, as soon as practicable. As part of the development and implementation, the following shall apply:

(i) Funding for information technology resources, projects and contracts shall be allocated to each Commonwealth agency by the office based on approved business case submissions.

(ii) Information technology budget codes and fund codes shall be created as required.

(3) The director shall develop strategic plans for information technology as necessary.

(c) Consultation and cooperation.--

(1) In determining whether a strategic plan is necessary for a State agency, the director shall consider the State agency's operational needs, functions and performance capabilities.

(2) The director shall consult with and assist State agencies in the preparation of plans under this subsection.

(3) Each State agency shall actively participate in preparing, testing and implementing an information technology plan as determined by the director. A State agency shall provide all financial information to the director necessary to determine full costs and expenditures for information technology assets, including resources provided by the State

agency or through contracts or grants.

(4) Each State agency shall prepare and submit plans as required by the director.

(5) A plan by a State agency shall be submitted to the director no later than October 1 of each even-numbered year.

(d) Biennial plan.--

(1) The director shall develop a biennial State Information Technology Plan, which shall be transmitted to the General Assembly in conjunction with the Governor's budget submission that year.

(2) The biennial plan shall include:

(i) An inventory of current information technology assets and major projects.

(ii) An inventory of significant unmet needs for information technology resources over a five-year time period, along with a ranking of the unmet needs in priority order according to their urgency.

(iii) A statement of the financial requirements, together with a recommended funding schedule for major projects in progress or anticipated for approval during the upcoming fiscal biennium.

(iv) An analysis of opportunities for Statewide initiatives that would yield significant efficiencies or improve effectiveness in State programs.

(3) As used in this subsection, the term "major project" includes a project costing more than $500,000 to implement.

§ 4316. Commonwealth Information Technology Fund.

(a) Establishment.--An account is established in the General Fund to be known as the Information Technology Fund.

(b) Receipt of money.--The fund shall receive money for the operations of the office and to fulfill the duties of the office under this chapter by the following methods:

(1) The transfer of encumbered funds from each State agency which were designated for information technology purposes prior to the effective date of this section.

(2) Transfers as authorized by the General Assembly that are not already provided for under this section.

(3) The transfer of a portion of a State agency's funds regarding general government operations for information technology employees.

(c) Use of fund money.--

(1) Subject to paragraph (2), the director shall approve the disbursement of money from the fund, which shall be used for the following purposes and other legitimate purposes:

(i) Project management.

(ii) Security.

(iii) E-mail operations for State agencies under the policy supervision and jurisdiction of the Governor.

(iv) State portal operations.

(v) State agencies' annual information technology budget.

(vi) Operations of the office, including salaries and expenses of all State agency information technology personnel.

(2) Expenditures for the operations of the office made from the fund that involve money appropriated from the General Fund shall be approved by the director.

§ 4317. Financial accountability and information technology.

(a) Development of processes.--Subject to subsection (b), the office, along with the Secretary of the Budget and the State Treasurer, shall develop processes for budgeting and accounting of expenditures for information technology operations, including all Commonwealth personnel, services, projects, infrastructure and assets across all State agencies.

(b) Included information.--The budgeting and accounting processes under subsection (a) shall include, but not be limited to, information regarding the following:

(1) Hardware.

(2) Software.

(3) Personnel.

(4) Training.

(5) Contractual services, including cloud service providers.

(6) Other items relevant to information technology.

(c) Significant resources.--State agency requests for significant resources shall provide the information required in section 4320 (relating to State agency requests for information technology and services).

(d) Reports generally.--Subject to subsections (e) and (f), by February 1 of each year, the director shall report to the General Assembly the following information:

(1) Services currently provided and associated transaction volumes or other relevant indicators of utilization by user type.

(2) New services added during the previous year.

(3) The total appropriation for each service.

(4) The total amount remitted to the vendor for each service.

(5) Any other use of State data by the vendor and the total amount of revenue collected per use and in total.

(6) User satisfaction with each service.

(7) Any other issues associated with the provision of each service.

(e) Financial information.--The director shall, at a minimum, include in the report under subsection (d) the following financial information:

(1) Current budgetary balances for the fund and each information technology project.

(2) Line-item details on expenditures.

(3) Anticipated expenditures for the next four years.

(4) Cybersecurity expenditures for the previous and next four years by each agency.

(5) The financial activities of the fund, including fund expenditures, during the immediately prior fiscal year.

(f) Issuance.--In addition to the General Assembly, a report under subsection (c) shall be submitted to the following:

(1) The Secretary of the Budget.

(2) The Independent Fiscal Office.

§ 4318. Commonwealth portal.

The office shall establish a single point of service accessible electronically by means in use by residents of this Commonwealth. The following shall apply:

(1) Each State agency shall functionally link its Internet or electronic services to a centralized web portal system established under this chapter.

(2) The office shall ensure the portal facilitates Commonwealth residents' ease in conducting online transactions with and obtaining information from State government.

(3) The portal shall be designed to facilitate and improve public interactions along with communications between State agencies.

§ 4319. Statewide information technology transparency portal.

(a) Implementation.--Within one year of the effective date of this chapter, the office shall develop, operate and update regularly a web-based portal detailing the status of each of the Commonwealth's information technology projects, to increase the transparency and convenience for the public in obtaining information regarding State information technology activity as contained in section 4317 (relating to financial accountability and information technology).

(b) Contents.--The portal shall include the following:

(1) A brief summary of each information technology project.

(2) The approved budget of each project.

(3) The total and percent of the project's approved budget that has been expended by the agency based on the end balance from the prior business day along with a color designation as follows:

(i) If an information technology project is under the project's approved budget, the project shall be designated as the color green.

(ii) If an information technology project is over the project's approved budget, the project shall be designated as the color red.

(4) The completion date in the original contract along with the total percent of work for the project that has been completed, along with a color designation as follows:

(i) If an information technology project has not exceeded the completion date in the original contract, the project shall be designated as the color green.

(ii) If an information technology project has exceeded the completion date in the original contract,

the project shall be designated as the color red.

(5) A summary of the scope of work along with a color designation as follows:

(i) If an information technology project is meeting the scope of work in the original contract, the project shall be designated as the color green.

(ii) If an information technology project is not meeting the scope of work in the original contract, the project shall be designated as the color red.

(6) A summary of the performance requirements of the contract, along with a color designation as follows:

(i) If an information technology project is meeting the performance requirements in the original contract, the project shall be designated as the color green.

(ii) If an information technology project is not meeting the performance measures in the original contract, the project shall be designated as the color red.

(c) Posting.--Posting of draft and final policy documents shall be made within 90 days of the effective date of this section.

(1) The office shall make available all proposed and existing information technology related policies and laws by an intranet accessible to all State employees.

(2) The policy intranet documents shall be made available via the web-based portal when deployed.

§ 4320. State agency requests for information technology and services.

A State agency shall submit a business case to the office, requesting significant resources as defined by the director, for the purpose of acquiring, operating or maintaining information technology or services for the State agency. The office shall supply sufficient staff support for agency business case development. The following shall apply regarding the business case:

(1) A review and evaluation shall be made of the business case that is prepared by the chief information officer assigned to the State agency that includes an assessment of risk and ensures that the cost and schedule estimates incorporate the risk assessment.

(2) In cases of an acquisition, there shall be an explanation of the method by which the acquisition is to be financed.

(3) A statement shall be made by the chief information officer assigned to the State agency that specifies viable alternatives, if any, for meeting the State agency needs in an economical and efficient manner. The statement shall include an analysis of alternatives that identifies the best approach for achieving mission improvement or program results within available funding and that takes into consideration the following:

(i) Organization, process and technology options.

(ii) At least three alternatives, including the status quo, a shared service or external service option and any other alternatives consistent with the architecture and strategy developed by the office.

(4) An assessment of and plan for ensuring cybersecurity and privacy issues shall be incorporated and funded in the request for resources.

§ 4321. Status of information technology projects and corrective action plans.

(a) Designation.--With respect to a business case under section 4320 (relating to State agency requests for information technology and services), the office shall designate as red, as specified under section 4319 (relating to Statewide information technology transparency portal), and identify a remediation plan, including contract and program restructuring, for programs experiencing cost or schedule overruns or performance shortfall exceeding the business case as funded. The following shall apply:

(1) The remediation plan and restructuring actions shall address root causes of the program and contract cost, performance or schedule overruns.

(2) The office shall ensure the business case is updated to establish a new baseline of cost, schedule and performance objectives that reflect the remediation plan and restructuring action.

(3) Upon determining that an information technology project has been designated red, the office shall notify the Governor's Office, the Auditor General and the General Assembly.

(4) The remediation plan and restructuring action shall be finalized within 60 days from notification.

(b) Transmittal.--The finalized corrective action plan shall be sent to the General Assembly and the Auditor General.

(c) Additional requirements.--The director shall notify the State Treasurer to suspend future expenditure of funds for any technology project that is designated as red under this section and that fails to adopt a remediation plan within the time outlined under this section. The following shall apply:

(1) If a State agency adopts within the time allowed under this section a remediation plan, but the project's designation remains red following implementation of the plan, the director shall require the agency to adopt a new remediation plan or may, at the director's discretion, suspend or terminate the project.

(2) To implement this section, the director and each State agency shall include as part of contract provisions necessary to suspend payment for the failure of a contractor or vendor to complete the requirements of the contract on time or on budget.

SUBCHAPTER C

BUSINESS OPERATIONS

Sec.
4331. Reporting requirements regarding procurement.
4332. Communications services.
4333. Project approval standards.
4334. Project management standards.
4335. Dispute resolution.
4336. Purchase of certain equipment prohibited.
4337. Refurbished computer equipment purchasing program.
4338. Data on reliability and other matters.

§ 4331. Reporting requirements regarding procurement.

(a) Bids.--A vendor submitting a bid or proposal shall disclose in a statement, provided contemporaneously with the bid or proposal, where services will be performed under the contract sought, including any subcontracts, and whether any services under that contract, including any subcontracts, are anticipated to be performed outside the United States.

(b) Retention and reports.--The director shall:

(1) Retain the statements required by this section regardless of the State agency that awards the contract.

(2) Report annually to the secretary on the number of contracts.

(c) Records of purchases.--Each State agency that makes a purchase of information technology through the office shall report directly to the director, who shall keep annual records of information technology purchases.

(d) Effect of section.--Nothing in this section is intended to contravene any existing treaty, law, agreement or regulation of the United States.

§ 4332. Communications services.

Except as otherwise provided under Subchapter G (relating to Pennsylvania Statewide Radio Network), the director shall exercise authority for telecommunications and other communications included in information technology relating to the internal management and operations of a State agency. In discharging this responsibility, the director shall:

(1) Ensure that no data of a confidential nature shall be entered into or processed through an information technology system or network established under this chapter until appropriate safeguards and other security measures are approved by the director and installed and fully operational.

(2) Provide for the establishment, management and operation, through State ownership, by contract or through commercial leasing, of the following systems and services as they affect the internal management and operation of State agencies:

(i) Central telephone systems and telephone networks, including Voice over Internet Protocol and commercial mobile radio systems.

(ii) Satellite services.

(iii) Closed-circuit television systems.

(iv) Two-way radio systems.

(v) Microwave systems.

(vi) Related systems based on telecommunication technologies.

(vii) Broadband.

(3) Coordinate the development of cost-sharing systems for respective State agencies for their proportionate parts of the cost of maintenance and operation of the systems and services listed in this section.

(4) Assist in the development of coordinated telecommunications services or systems within and among all State agencies and recommend, where appropriate, cooperative utilization of telecommunication facilities by aggregating users.

(5) Perform traffic analysis and engineering for all telecommunications services and systems listed in this section.

(6) Establish telecommunications specifications and designs so as to promote and support compatibility of the systems within State agencies.

(7) Provide every three years an inventory of telecommunications costs, facilities, systems and personnel within State agencies.

(8) Promote, coordinate and assist in the design and engineering of emergency telecommunications systems, including, but not limited to, the 911 emergency telephone number program, emergency medical services and other emergency telecommunications services.

(9) Perform frequency coordination and management for State agencies and municipalities, in accordance with the rules and regulations of the Federal Communications Commission or any successor Federal agency.

(10) Advise all State agencies on telecommunications management planning and related matters and provide opportunities for training to users within State agencies in telecommunications technology and systems.

(11) Assist and coordinate the development of policies and long-range plans, consistent with the protection of residents' rights to privacy and access to information, for the acquisition and use of telecommunications systems. All policies and plans shall be based on current information about the Commonwealth's telecommunications activities in relation to the full range of emerging technologies.

§ 4333. Project approval standards.

(a) Review and approval.--The director shall review all proposed information technology projects for each State agency and make a determination of approval or disapproval within 15 business days of receipt. Project approval may be granted upon the director's determination that:

(1) the project conforms to project management procedures and policies and to procurement rules and

policies; and

(2) sufficient funds are available for implementation.

(b) Implementation.--Unless expressly exempt within this chapter, a State agency may not proceed with an information technology project until the director approves the project.

(c) Disapproval.--If a project is not approved, the director shall specify in writing the grounds for the disapproval after making the determination. The director shall provide notice of the disapproval, along with the grounds for the disapproval, to all of the following:

(1) The State agency.

(2) The Secretary of the Budget.

(3) The State Treasurer.

(4) The Auditor General.

(5) The General Assembly.

(d) Suspension.--

(1) The director may suspend an information technology project if the project:

(i) fails to meet the applicable quality assurance standards;

(ii) has exceeded its projected costs; or

(iii) has failed to meet its projected completion date.

(2) If the director suspends a project for a reason under paragraph (1), the director shall specify in writing the grounds for suspending the project no later than five business days after making the determination. The director shall provide notice of the suspension, along with the grounds for suspension, to all of the following:

(i) The State agency.

(ii) The Secretary of the Budget.

(iii) The State Treasurer.

(iv) The Auditor General.

(v) The General Assembly.

(vi) Any vendor or organization contracted by the respective State agency for work on the suspended project.

(3) After a project has been suspended, the State Treasurer may not allow the transfer of money from the State agency to support additional work under the project unless the director approves an amended version of the plan for the project.

(4) If a State agency attempts to continue to implement a project that is no longer approved by the director and expend additional money for the project, the State Treasurer shall prevent the transfer of funds and remit the intended expenditures into the fund. After remitting the unauthorized expenditure, the State Treasurer shall immediately notify the following:

(i) The director.

(ii) The Governor.

(iii) The Secretary of the Budget.

(iv) The General Assembly.

§ 4334. Project management standards.

(a) Personnel.--Each State agency shall provide personnel if necessary to participate in project management, implementation, testing and other activities for an information technology project.

(b) Policies.--The director shall develop office policies for implementing an approved project, whether the project is undertaken in single or multiple phases or components.

(c) Project management assistant.--

(1) The director may designate a project management assistant to implement an information technology project of a State agency.

(2) A project management assistant for a State agency shall:

(i) Advise the State agency regarding the initial planning of an information technology project, the content and design of a request for proposals, contract development, procurement and architectural and other technical reviews.

(ii) Monitor progress in the development and implementation of an information technology project.

(iii) Provide status reports to the State agency and the director, including recommendations regarding continued approval of an information technology project.

(3) Personnel of the State agency to which a project management assistant is designated shall provide periodic reports to the project management assistant regarding an information technology project. Each report shall include information regarding the following:

(i) The State agency's business requirements.

(ii) Applicable laws and regulations.

(iii) Project costs.

(iv) Issues related to hardware, software or training.

(v) Projected and actual completion dates for the project.

(vi) Any other information related to the implementation of the project.

§ 4335. Dispute resolution.

(a) Right to request for review.--If the director has disapproved or suspended an information technology project or has disapproved a State agency's request for an amended version of the plan for the project, the affected State agency may request the director to revisit the determination about the project. The request for review shall be submitted in writing to the director within 15 business days following the State agency's receipt of the disapproval or suspension.

(b) Contents of request for review.--A request for review under subsection (a) shall specify the grounds for the State

agency's disagreement with the director's determination. The State agency shall include with its request a plan to modify the project to meet the director's concerns.

(c) Notification.--

(1) Within 30 days after initial receipt of a State agency's request for review, the director shall notify the State agency whether or not the project, as modified, may be implemented.

(2) If the director approves the implementation of a modified project by a State agency, the director shall notify the State Treasurer and the Secretary of the Budget immediately. The State agency shall notify all contracted third parties of any changes or modifications to the project.

§ 4336. Purchase of certain equipment prohibited.

(a) Determination.--A State agency may not purchase information technology equipment or televisions, or enter into a contract with a manufacturer, unless the director determines that the purchase or contract is in compliance with the requirements under this chapter and existing State law regarding the procurement of information technology equipment and televisions.

(b) Findings.--If the director determines that a purchase or contract is not in compliance with the requirements under this chapter or existing State law regarding the procurement of information technology equipment and televisions, the director shall issue written findings regarding the noncompliance to the State agency.

§ 4337. Refurbished computer equipment purchasing program.

(a) Option.--The office shall offer a State agency the option of purchasing, leasing or using refurbished computer equipment from registered computer equipment refurbishers whenever most appropriate to meet the respective needs of the State agency.

(b) Savings.--A State agency shall document any savings resulting from the purchase of refurbished computer equipment, including, but not limited to, the initial acquisition cost and operations and maintenance costs. The savings shall be reported annually to:

(1) The director.

(2) The General Assembly.

(c) Requirements.--Participating computer equipment refurbishers shall meet all existing procurement requirements established by the office.

§ 4338. Data on reliability and other matters.

(a) Maintenance of data.--The office shall maintain data on equipment reliability, potential cost savings and matters associated with the refurbished computer equipment purchasing program.

(b) Report.--The office shall transmit a report regarding the matters under subsection (a) by February 1, 2020, and quarterly thereafter to:

(1) The Secretary of the Budget.
(2) The Independent Fiscal Office.
(3) The General Assembly.

SUBCHAPTER D
PROCUREMENT OF INFORMATION TECHNOLOGY

Sec.
4345. Duties of office.
4346. Confidentiality.
4347. Methods of procurement.
4348. Quality assurance.

§ 4345. Duties of office.

(a) Specific duties of office.--Subject to the provisions of this chapter and consistent with the processes enacted under 62 Pa.C.S. Ch. 5 (relating to source selection and contract formation), the office shall have the authority and responsibility to:

(1) Contract for all information technology and information technology as a service for State agencies. The office may enter into purchase orders under this type of contract.

(2) Establish processes, specifications and standards that shall apply to all information technology to be purchased, licensed or leased by State agencies.

(3) Establish processes, specifications and standards relating to information technology services contract requirements for State agencies.

(4) Utilize the purchasing benchmarks established by the director.

(5) Provide strategic sourcing resources and planning to compile and consolidate all estimates of information technology goods and services needed and required by State agencies.

(6) Ensure, to the maximum extent practicable, that projects utilize Statements of Objectives when issuing solicitations for information technology projects that are for noncommodity hardware. The following shall apply:

(i) As used in this paragraph, the term "Statement of Objective" means an office-prepared or State-agency-prepared document incorporated into the solicitation that states the overall performance objectives or outcomes of the project.

(ii) A Statement of Objective shall be used in solicitations when the office or State agency intends to provide the maximum flexibility to each offeror to propose an innovative approach.

(iii) A Statement of Objective may be used in lieu of a detailed statement of work that dictates detailed requirements that stifle flexible, innovation solutions.

(b) Specific duties of State agencies.--Subject to the provisions of this chapter and consistent with the processes enacted under 62 Pa.C.S. Ch. 5, each State agency shall have the

authority and responsibility to issue purchase orders under contracts entered by the office.

§ 4346. Confidentiality.

(a) Contract information.--Subject to subsection (b), contract information compiled by the office shall be made a matter of public record after the award of contract.

(b) Proprietary information.--Trade secrets, test data and similar proprietary information and security information protected from disclosure under Federal or State law shall remain confidential.

§ 4347. Methods of procurement.

(a) Electronic procurement.--

(1) The office may authorize the use of an electronic procurement system to conduct a reverse auction and electronic bidding on existing multiple-award contracts.

(2) The following shall apply regarding reverse auctions:

(i) The vendor's price may be revealed during the reverse auction.

(ii) The office may contract with a third-party vendor to conduct the reverse auction.

(iii) Offers or bids may be accepted and contracts may be entered by use of electronic bidding.

(iv) All requirements relating to formal and competitive bids, including advertisement, seal and signature, are satisfied when a procurement is conducted or a contract is entered in compliance with the reverse auction or electronic bidding requirements established by the office.

(v) The office shall limit the use of reverse auctions in procurement of information technology to the acquisition of information technology hardware.

(vi) The office shall not use reverse auctions for the procurement of information technology services, hardware software or solutions that incorporate both information technology hardware and services, including, but not limited to, cloud-based information technology solutions.

(3) As used in this subsection, "existing multiple-award contracts" means one or more contracts where the same or similar goods are being procured by State agencies.

(b) Bulk purchasing.--

(1) The director shall establish procedures for the procurement of information technology through bulk purchases. The procedures may include the following:

(i) The aggregation of hardware purchases.

(ii) The use of formal bid procedures.

(iii) Restrictions on supplemental staffing.

(iv) Enterprise software licensing, hosting and multiyear maintenance agreements.

(v) Information technology as a service.

(2) The director may require State agencies to submit information technology procurement requests to the department on October 1, January 1 and June 1, or another regularly occurring schedule, of each fiscal year in order to allow for bulk purchasing.

(c) Most advantageous offer.--All bids or offers to contract, whether through competitive sealed bidding or other procurement method under 62 Pa.C.S. Ch. 5 (relating to source selection and contract formation), shall be subject to evaluation and selection by acceptance of the most advantageous offer to the Commonwealth.

(d) Considerations.--Evaluation of an information technology purchase shall take into consideration the following factors:

(1) The best value of the purchase.

(2) Compliance with information technology project management policies.

(3) Compliance with information technology security standards and policies.

(4) Substantial conformity with the specifications and other conditions set forth in the solicitation.

(e) Exceptions.--In addition to permitted waivers of competition, the requirements of competitive bidding shall not apply to information technology contracts and procurements:

(1) in the case of a pressing need or an emergency arising from an information technology security incident; or

(2) in the use of master licensing or purchasing agreements governing the office's acquisition of proprietary intellectual property.

(f) Award by director.--The director may award a cost plus percentage of cost contract for information technology projects. As needed, the director shall report the cost plus percentage of cost contract to the following:

(1) The Secretary of the Budget.

(2) The Auditor General.

(3) The General Assembly.

§ 4348. Quality assurance.

Information technology projects authorized under this chapter shall meet all project standards and requirements established under this chapter.

SUBCHAPTER E
SECURITY

Sec.
4351. Statewide security standards.
4352. Security standards and risk assessments.
4353. Assessment of compliance with security standards.
4354. Joint Cybersecurity Oversight Committee.

§ 4351. Statewide security standards.

(a) Establishment.--

(1) The director shall establish a Statewide set of standards for information technology security to maximize the functionality, security and interoperability of the

Commonwealth's distributed information technology assets, including:

(i) Data classification.

(ii) Management.

(iii) Communications.

(iv) Encryption technologies.

(2) The standards under this subsection shall conform to the industry's best practices and standards regarding information technology security.

(b) Review and revision.--The director shall review and revise the security standards annually as necessary. As part of this function, the director shall review periodically existing security standards and practices in place among the various State agencies to determine whether those standards and practices meet Statewide security and encryption requirements.

(c) Assumption of responsibilities.--The director may assume the direct responsibility of providing for the information technology security of a State agency that fails to adhere to security standards adopted under this chapter.

§ 4352. Security standards and risk assessments.

(a) Authorization to operate.--Notwithstanding any other provision of law and except as otherwise provided by this chapter, all information technology security goods, software or services purchased using taxpayer money, or for use by a State agency or in a public facility, shall require an authorization to operate by the head of the State agency in accordance with security standards under this chapter. No information technology system or service may be operated by, or in support of, a State agency without an authorization to operate.

(b) Standards.--The director shall define a risk-based set of control standards that identify specific security and privacy protections for all information technology and information technology services in line with the specific threats and risks to the residents of this Commonwealth and State agency operations.

(c) Assessments.--The director shall conduct risk assessments to identify compliance and operational and strategic risks to the information technology network and agency operations. The following shall apply:

(1) The assessments may include methods such as penetration testing, social engineered security threats or similar assessment methodologies.

(2) The director may contract with another party to perform the assessments.

(3) The following assessment reviews shall be performed prior to the information security audit under subsection (e) and the assessment shall be performed consistent with the Federal information processing standards:

(i) Identity management.

(ii) Security incident management.

(iii) Network perimeter security.

(iv) Systems development.
(v) Project management.
(vi) Information technology risk management.
(vii) Data management.
(viii) Vulnerability management.
(4) Detailed reports of the risk and security issues identified in the assessments shall be reported to the director and shall be kept confidential.
(5) The agency head, in consultation with the office, shall identify corrective or mitigating actions as needed.
(d) Interim authority to operate.--If the agency head determines that the information technology system or service is needed, the agency head may seek authorization from the director for a period not longer than 180 days to implement the corrective or mitigating actions.
(e) Security audit.--
(1) The director shall contract with an independent certified information security auditor or entity to perform an information security audit of State agencies.
(2) The director shall determine a schedule for continuous State agency information security audits.
(f) Notification and audits.--The following shall apply:
(1) The party conducting the assessment or audit shall provide the director and head of the reviewed State agency with a detailed report of the security issues identified, which shall not be publicly disclosed.
(2) The State agency, in cooperation with the office, shall provide the director with a corrective action plan that remediates issues identified in the detailed report under paragraph (1), which shall not be publicly disclosed.
(3) The director shall issue a public report on the general results of the assessment that shall be accessible on the portal under section 4319 (relating to Statewide information technology transparency portal).
(g) Effect of section.--Nothing in this section shall be construed to preclude the Auditor General or the General Assembly from assessing the security practices of State information technology systems as part of its statutory duties and responsibilities.
§ 4353. Assessment of compliance with security standards.
(a) Frequency.--The director shall biannually assess the ability of each State agency's contracted vendors to comply with the current security standards established under this chapter.
(b) Contents.--The director shall establish a quantifiable objective metric that measures the degree of compliance with current security standards. The assessment under this section shall, at a minimum:
(1) Quantify the degree of compliance with the current security standards using the metric.
(2) Include security organization, security practices, security information standards, network security

architecture, systems development and lifecycle management and current expenditures of State funds for information security.

(3) Include an estimate of the cost to implement the security measures needed for State agencies to fully comply with the established standards.

(c) Submittal of information.--Each State agency shall submit information required by the director for the assessments under this section.

§ 4354. Joint Cybersecurity Oversight Committee.

(a) Establishment and membership.--The Joint Cybersecurity Oversight Committee is established and shall consist of the following members:

(1) The director.

(2) The following individuals appointed by the President pro tempore of the Senate:

(i) Two members of the Senate.

(ii) A representative from the Information Technology Office of the majority caucus of the Senate.

(3) The following individuals appointed by the Minority Leader of the Senate:

(i) One member of the Senate.

(ii) A representative from the Information Technology Office of the minority caucus of the Senate.

(4) The following individuals appointed by the Speaker of the House of Representatives:

(i) Two members of the House of Representatives.

(ii) A representative from the Information Technology Office of the majority caucus of the House of Representatives.

(5) The following individuals appointed by the Minority Leader of the House of Representatives:

(i) One member of the House of Representatives.

(ii) A representative from the Information Technology Office of the minority caucus of the House of Representatives.

(6) The Attorney General or a designee of the Attorney General.

(7) The chief information officer of:

(i) The Department of the Auditor General.

(ii) The Treasury Department.

(iii) The Office of Attorney General.

(iv) The Administrative Office of Pennsylvania Courts.

(v) The Pennsylvania Public Utility Commission.

(8) Four private citizens appointed by the Governor with professional cybersecurity experience.

(9) The Commissioner of the Pennsylvania State Police or a designee of the commissioner.

(10) A member of the National Guard experienced in cybersecurity, as appointed by the Adjutant General.

(b) Chairperson and vice chairperson.--The chairperson of the committee shall be appointed by the Governor, and the vice chairperson of the committee shall be appointed by the chairperson.

(c) Staffing.--

(1) The committee shall be staffed by the office, which shall support and assist the committee.

(2) Costs incurred for mileage for a member shall be reimbursed by the individual or entity appointing the member.

(d) Service of members.--Each member of the committee shall serve at the pleasure of the individual who appointed the member.

(e) Vacancies.--A vacancy in the membership of the committee shall be filled by the appointing authority in the same manner as the original appointment.

(f) Meetings.--

(1) The committee shall meet at least on a quarterly basis and no later than the first Thursday of each quarter.

(2) The chairperson of the committee, with the consent of the vice chairperson of the committee, may schedule additional meetings of the committee.

(3) The chairperson of the committee shall provide the members of the committee with notice of the time and location of each meeting of the committee no later than one week prior to the meeting. Notice shall also be provided to the Governor, the President pro tempore of the Senate and the Speaker of the House of Representatives.

(4) Notice of the meetings of the committee shall be provided by regular mail and e-mail.

(5) A member of the committee may participate in a meeting of the committee in person, by teleconference, by video conference or by other means as agreed to by the chairperson and vice chairperson of the committee.

(6) A meeting of the committee shall not be subject to 65 Pa.C.S. Ch. 7 (relating to open meetings).

(7) A meeting held by the Committee in which the committee accepts testimony shall comply with 65 Pa.C.S. Ch. 7.

(g) Duties.--

(1) The committee shall review and coordinate cybersecurity policies and discuss emerging cybersecurity threats, recommended policy changes and assess current cybersecurity within this Commonwealth.

(2) The committee shall prepare a report of its activities, which shall be transmitted to the following:

(i) The Governor.

(ii) The President pro tempore of the Senate.

(iii) The Speaker of the House of Representatives.

(iv) The Majority Leader and the Minority Leader of the Senate.

(v) The Majority Leader and the Minority Leader of

the House of Representatives.

(vi) The Court Administrator of Pennsylvania.

(h) Definitions.--As used in this section, the following words and phrases shall have the meanings given to them in this subsection unless the context clearly indicates otherwise:

"Committee." The Joint Cybersecurity Oversight Committee established under this section.

SUBCHAPTER F

ENFORCEMENT AND PENALTIES

Sec.

§ 4361. Administrative and judicial review.

Actions taken by the director under this chapter shall be subject to review in accordance with 2 Pa.C.S. Chs. 5 (relating to practice and procedure) and 7 (relating to judicial review).

§ 4362. Unauthorized use for private benefit prohibited.

(a) Offense.--It is unlawful for any person, by the use of the powers, policies or procedures, to purchase, attempt to purchase, procure or attempt to procure any property or services for private use or benefit.

(b) Criminal penalties and fines.--A person that violates subsection (a) commits a misdemeanor of the first degree. Upon conviction, the person shall be liable to the Commonwealth to repay any amount expended in violation of this chapter, together with any court costs.

§ 4363. Financial interests.

(a) Offense.--

(1) The director, any other policymaking employee of the office and any employee of a State agency involved in management or oversight, including contract administration, of the information technology project may not have a financial interest or personal beneficial interest, either directly or indirectly, in the purchase of or contract for information technology. The financial interest or personal interest shall extend to a corporation, partnership, company, trust, association or other entity furnishing information technology to the Commonwealth or any of its State agencies.

(2) An official covered in paragraph (1) may not accept or receive, directly or indirectly, any of the following:

(i) Anything of monetary or other value, whether by rebate, gift or otherwise.

(ii) A promise, obligation or contract for future reward, employment or compensation, regardless of the business or nonbusiness nature of the promise, obligation or contract.

(b) Criminal penalties.--A person that violates subsection (a) commits a felony of the third degree. Upon conviction, the person shall be removed from office or State employment.

§ 4364. Certification of submittal without collusion.

(a) Duty.--The director shall require bidders under this chapter to certify that each bid on information technology contracts overseen by the office is submitted competitively and without collusion.

(b) Grading.--A person that provides a false certification under this section commits a misdemeanor of the first degree.

Subchapter G
Pennsylvania Statewide Radio Network

Sec.

§ 4371. Definitions.

The following words and phrases when used in this subchapter shall have the meanings given to them in this section unless the context clearly indicates otherwise:

"Business partner." An organization that has entered into an agreement with the Commonwealth under which it offers some form of nonmonetary consideration, such as frequency licenses or sites for system infrastructure, in return for permission to use PA-STARNet for radio communications.

"Commissioner." The Commissioner of Pennsylvania State Police.

"Committee." The PA-STARNet Committee established under § 4373 (relating to PA-STARNet Committee).

"Emergency communications." The means and methods for exchanging communications and information necessary for successful incident management.

"First responder." An individual who in the early stages of an incident is responsible for the protection and preservation of life, property, evidence and the environment, including emergency response providers as that term is defined in section 2 of the Homeland Security Act of 2002 (Public Law 107-296, 116 Stat. 2135).

"Participating agency." A government agency, public safety organization, first responder organization, business partner or other organization.

"Pennsylvania Statewide Radio Network" or "PA-STARNet." A Statewide radio network comprising a communication and information infrastructure connected by a digital microwave system for transmission of voice and data, including all frequency bands and other system extensions owned and operated by the Commonwealth and connected to the core digital trunked radio network operating in the 800 megahertz (MHz) public safety frequency band and in other public safety frequency bands licensed by the Federal Communications Commission (FCC), or to the microwave backbone network.

"Public safety communications." The means and methods for transmitting and receiving information necessary for the conduct of services rendered by or through Federal, State or local

government entities in support of the protection and preservation of life, property and natural resources, as prescribed by law.

"State police." The Pennsylvania State Police.

§ 4372. Administration of PA-STARNet.

(a) Authority.--The State police, through a PA-STARNet division, shall develop, operate, regulate, manage, maintain and monitor PA-STARNet, including PA-STARNet infrastructure, equipment, software, services and licenses.

(b) Purposes.--The State police shall administer PA-STARNet for:

(1) the benefit of the participating agencies;

(2) the support of effective communications at critical public events; and

(3) the interoperable communication needs of Federal, State and local first responders during emergencies.

(c) Policies and procedures.--The State police shall establish policies and procedures for the specification, procurement, development, testing, configuration, operations, use, replacement and maintenance of PA-STARNet resources.

§ 4373. PA-STARNet Committee.

The PA-STARNet Committee is established in the State police to provide a standing forum for participating agencies to ensure coordination and cooperation among participating State agencies and county and local agencies in the development and use of PA-STARNet and its application to public safety communications and emergency communications.

Section 2. This act shall take effect immediately.