

AMENDMENTS TO HOUSE BILL NO. 40

Sponsor: REPRESENTATIVE RYAN

Printer's No. 19

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

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

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

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

17 CHAPTER 43

18 INFORMATION TECHNOLOGY

19 Subchapter

20 A. General Provisions

21 B. Office of Information Technology

22 C. Business Operations

23 D. Procurement of Information Technology

24 E. Security

25 F. Enforcement and Penalties

26 G. Pennsylvania Statewide Radio Network

27 SUBCHAPTER A

28 GENERAL PROVISIONS

29 Sec.

30 4301. Scope of chapter.

31 4302. Findings and declarations.

32 4303. Definitions.

33 § 4301. Scope of chapter.

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

1 § 4302. Findings and declarations.

2 The General Assembly finds and declares the following:

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

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

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

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

18 (5) By reforming the Commonwealth's outdated approach to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

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

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

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

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

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

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

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

43 § 4303. Definitions.

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

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

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

1 (1) authorizes operation of a product and explicitly
2 accepts the risk to agency operations; and
3 (2) is signed after the system has met and passed all
4 requirements to become operational.

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

12 (1) The State's current technology.

13 (2) The opportunities for technology sharing.

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

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

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

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

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

29 "Independent agency." As follows:

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

33 (2) The term does not include:

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

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

38 "Independent department." Any of the following:

39 (1) The Department of the Auditor General.

40 (2) The Treasury Department.

41 (3) The Office of Attorney General.

42 (4) A board or commission of an entity under paragraph
43 (1), (2) or (3).

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

47 (1) Personal computers.

48 (2) Servers.

49 (3) Mainframes.

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

51 (5) Broadband.

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

15 "Information technology budget." As follows:

16 (1) All information technology expenditures listed by
17 project and amount of expenditure for planning, development,
18 modernization, operations and maintenance.

19 (2) The term includes all software, hardware,
20 Commonwealth and vendor staff and service costs.

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

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

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

35 "Portal." A publicly available Internet website.

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

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

41 "State agency." Any of the following:

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

48 SUBCHAPTER B

49 OFFICE OF INFORMATION TECHNOLOGY

50 Sec.

51 4311. Establishment of office.

4312. Duties of office.
4313. Director.
4314. Transfer of additional duties and personnel.
4315. Planning and financing information technology resources.
4316. Commonwealth Information Technology Fund.
4317. Financial accountability and information technology.
4318. Commonwealth portal.
4319. Statewide information technology transparency portal.
4320. State agency requests for information technology and
services.
4321. Status of information technology projects and corrective
action plans.

§ 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.

1 (iv) Defining information technology organization
2 and relationships.
3 (v) Managing information technology investment.
4 (vi) Communicating management aims and direction.
5 (vii) Managing information technology human
6 resources.
7 (viii) Managing quality.
8 (ix) Assessing risks.
9 (x) Managing projects.
10 (xi) Identifying automated solutions.
11 (xii) Acquiring and maintaining application
12 software.
13 (xiii) Acquiring and maintaining technology
14 infrastructure.
15 (xiv) Enabling operation and use.
16 (xv) Procuring information technology resources.
17 (xvi) Managing changes.
18 (xvii) Installing and accrediting solutions and
19 changes.
20 (xviii) Defining and managing service levels.
21 (xix) Managing third-party services.
22 (xx) Managing performance and capacity.
23 (xxi) Ensuring continuous service.
24 (xxii) Ensuring system security.
25 (xxiii) Identifying and allocating costs.
26 (xxiv) Educating and training users.
27 (xxv) Managing service desk and incidents.
28 (xxvi) Managing the configuration.
29 (xxvii) Managing problems.
30 (xxviii) Managing data.
31 (xxix) Managing physical environment.
32 (xxx) Managing operations.
33 (xxxii) Monitoring and evaluating information
34 technology performance.
35 (xxxiii) Monitoring and evaluating internal controls.
36 (xxxiv) Ensuring compliance with external
37 requirements.
38 (xxxv) Providing improved information technology
39 governance.

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

- 42 (1) Develop and administer a comprehensive long-range
43 plan to ensure the proper management of the information
44 technology resources of the Commonwealth.
45 (2) Set technical standards for information technology
46 and review and approve information technology projects and
47 budgets.
48 (3) Establish information technology security standards.
49 (4) Provide for the procurement of information
50 technology resources.
51 (5) Develop a schedule for the replacement or

1 modification of information technology systems.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

47 (34) Develop and produce cost, risk and quality
48 initiatives that consolidate State agency information
49 technology services, including, but not limited to,
50 infrastructure, personnel, investments, operations and
51 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

1 measurably improves Commonwealth agency mission
2 effectiveness.

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

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

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

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

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

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

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

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

26 § 4313. Director.

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

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

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

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

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

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

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

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

1 red in accordance with section 4321 (relating to status of
2 information technology projects and corrective action plans).
3 (d) Oversight.--The director shall oversee the manner and
4 means by which information technology business and disaster
5 recovery plans for State agencies are created, reviewed and
6 updated.

7 (e) Disaster recovery plan.--

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

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

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

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

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

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

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

29 § 4314. Transfer of additional duties and personnel.

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

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

37 (i) Report directly to the director.

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

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

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

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

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

7 § 4315. Planning and financing information technology
8 resources.

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

13 (b) Development of plan.--

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

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

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

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

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

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

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

39 (c) Consultation and cooperation.--

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

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

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

1 agency or through contracts or grants.

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

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

6 (d) Biennial plan.--

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

11 (2) The biennial plan shall include:

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

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

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

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

25 (3) As used in this subsection, the term "major project"
26 includes a project costing more than \$500,000 to implement.
27 § 4316. Commonwealth Information Technology Fund.

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

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

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

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

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

41 (c) Use of fund money.--

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

45 (i) Project management.

46 (ii) Security.

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

49 (iv) State portal operations.

50 (v) State agencies' annual information technology
51 budget.

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

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

7 § 4317. Financial accountability and information technology.

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

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

17 (1) Hardware.

18 (2) Software.

19 (3) Personnel.

20 (4) Training.

21 (5) Contractual services, including cloud service
22 providers.

23 (6) Other items relevant to information technology.

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

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

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

34 (2) New services added during the previous year.

35 (3) The total appropriation for each service.

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

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

40 (6) User satisfaction with each service.

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

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

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

48 (2) Line-item details on expenditures.

49 (3) Anticipated expenditures for the next four years.

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

1 (5) The financial activities of the fund, including fund
2 expenditures, during the immediately prior fiscal year.
3 (f) Issuance.--In addition to the General Assembly, a report
4 under subsection (c) shall be submitted to the following:
5 (1) The Secretary of the Budget.
6 (2) The Independent Fiscal Office.
7 § 4318. Commonwealth portal.
8 The office shall establish a single point of service
9 accessible electronically by means in use by residents of this
10 Commonwealth. The following shall apply:
11 (1) Each State agency shall functionally link its
12 Internet or electronic services to a centralized web portal
13 system established under this chapter.
14 (2) The office shall ensure the portal facilitates
15 Commonwealth residents' ease in conducting online
16 transactions with and obtaining information from State
17 government.
18 (3) The portal shall be designed to facilitate and
19 improve public interactions along with communications between
20 State agencies.
21 § 4319. Statewide information technology transparency portal.
22 (a) Implementation.--Within one year of the effective date
23 of this chapter, the office shall develop, operate and update
24 regularly a web-based portal detailing the status of each of the
25 Commonwealth's information technology projects, to increase the
26 transparency and convenience for the public in obtaining
27 information regarding State information technology activity as
28 contained in section 4317 (relating to financial accountability
29 and information technology).
30 (b) Contents.--The portal shall include the following:
31 (1) A brief summary of each information technology
32 project.
33 (2) The approved budget of each project.
34 (3) The total and percent of the project's approved
35 budget that has been expended by the agency based on the end
36 balance from the prior business day along with a color
37 designation as follows:
38 (i) If an information technology project is under
39 the project's approved budget, the project shall be
40 designated as the color green.
41 (ii) If an information technology project is over
42 the project's approved budget, the project shall be
43 designated as the color red.
44 (4) The completion date in the original contract along
45 with the total percent of work for the project that has been
46 completed, along with a color designation as follows:
47 (i) If an information technology project has not
48 exceeded the completion date in the original contract,
49 the project shall be designated as the color green.
50 (ii) If an information technology project has
51 exceeded the completion date in the original contract,

1 the project shall be designated as the color red.

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

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

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

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

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

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

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

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

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

27 § 4320. State agency requests for information technology and
28 services.

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

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

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

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

1 (i) Organization, process and technology options.
2 (ii) At least three alternatives, including the
3 status quo, a shared service or external service option
4 and any other alternatives consistent with the
5 architecture and strategy developed by the office.
6 (4) An assessment of and plan for ensuring cybersecurity
7 and privacy issues shall be incorporated and funded in the
8 request for resources.
9 § 4321. Status of information technology projects and
10 corrective action plans.
11 (a) Designation.--With respect to a business case under
12 section 4320 (relating to State agency requests for information
13 technology and services), the office shall designate as red, as
14 specified under section 4319 (relating to Statewide information
15 technology transparency portal), and identify a remediation
16 plan, including contract and program restructuring, for programs
17 experiencing cost or schedule overruns or performance shortfall
18 exceeding the business case as funded. The following shall
19 apply:
20 (1) The remediation plan and restructuring actions shall
21 address root causes of the program and contract cost,
22 performance or schedule overruns.
23 (2) The office shall ensure the business case is updated
24 to establish a new baseline of cost, schedule and performance
25 objectives that reflect the remediation plan and
26 restructuring action.
27 (3) Upon determining that an information technology
28 project has been designated red, the office shall notify the
29 Governor's Office, the Auditor General and the General
30 Assembly.
31 (4) The remediation plan and restructuring action shall
32 be finalized within 60 days from notification.
33 (b) Transmittal.--The finalized corrective action plan shall
34 be sent to the General Assembly and the Auditor General.
35 (c) Additional requirements.--The director shall notify the
36 State Treasurer to suspend future expenditure of funds for any
37 technology project that is designated as red under this section
38 and that fails to adopt a remediation plan within the time
39 outlined under this section. The following shall apply:
40 (1) If a State agency adopts within the time allowed
41 under this section a remediation plan, but the project's
42 designation remains red following implementation of the plan,
43 the director shall require the agency to adopt a new
44 remediation plan or may, at the director's discretion,
45 suspend or terminate the project.
46 (2) To implement this section, the director and each
47 State agency shall include as part of contract provisions
48 necessary to suspend payment for the failure of a contractor
49 or vendor to complete the requirements of the contract on
50 time or on budget.

51 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.

1 (iv) Two-way radio systems.
2 (v) Microwave systems.
3 (vi) Related systems based on telecommunication
4 technologies.
5 (vii) Broadband.
6 (3) Coordinate the development of cost-sharing systems
7 for respective State agencies for their proportionate parts
8 of the cost of maintenance and operation of the systems and
9 services listed in this section.
10 (4) Assist in the development of coordinated
11 telecommunications services or systems within and among all
12 State agencies and recommend, where appropriate, cooperative
13 utilization of telecommunication facilities by aggregating
14 users.
15 (5) Perform traffic analysis and engineering for all
16 telecommunications services and systems listed in this
17 section.
18 (6) Establish telecommunications specifications and
19 designs so as to promote and support compatibility of the
20 systems within State agencies.
21 (7) Provide every three years an inventory of
22 telecommunications costs, facilities, systems and personnel
23 within State agencies.
24 (8) Promote, coordinate and assist in the design and
25 engineering of emergency telecommunications systems,
26 including, but not limited to, the 911 emergency telephone
27 number program, emergency medical services and other
28 emergency telecommunications services.
29 (9) Perform frequency coordination and management for
30 State agencies and municipalities, in accordance with the
31 rules and regulations of the Federal Communications
32 Commission or any successor Federal agency.
33 (10) Advise all State agencies on telecommunications
34 management planning and related matters and provide
35 opportunities for training to users within State agencies in
36 telecommunications technology and systems.
37 (11) Assist and coordinate the development of policies
38 and long-range plans, consistent with the protection of
39 residents' rights to privacy and access to information, for
40 the acquisition and use of telecommunications systems. All
41 policies and plans shall be based on current information
42 about the Commonwealth's telecommunications activities in
43 relation to the full range of emerging technologies.
44 § 4333. Project approval standards.
45 (a) Review and approval.--The director shall review all
46 proposed information technology projects for each State agency
47 and make a determination of approval or disapproval within 15
48 business days of receipt. Project approval may be granted upon
49 the director's determination that:
50 (1) the project conforms to project management
51 procedures and policies and to procurement rules and

1 policies; and

2 (2) sufficient funds are available for implementation.

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

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

11 (1) The State agency.

12 (2) The Secretary of the Budget.

13 (3) The State Treasurer.

14 (4) The Auditor General.

15 (5) The General Assembly.

16 (d) Suspension.--

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

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

21 (ii) has exceeded its projected costs; or

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

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

30 (i) The State agency.

31 (ii) The Secretary of the Budget.

32 (iii) The State Treasurer.

33 (iv) The Auditor General.

34 (v) The General Assembly.

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

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

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

50 (i) The director.

51 (ii) The Governor.

1 (iii) The Secretary of the Budget.
2 (iv) The General Assembly.
3 § 4334. Project management standards.
4 (a) Personnel.--Each State agency shall provide personnel if
5 necessary to participate in project management, implementation,
6 testing and other activities for an information technology
7 project.
8 (b) Policies.--The director shall develop office policies
9 for implementing an approved project, whether the project is
10 undertaken in single or multiple phases or components.
11 (c) Project management assistant.--
12 (1) The director may designate a project management
13 assistant to implement an information technology project of a
14 State agency.
15 (2) A project management assistant for a State agency
16 shall:
17 (i) Advise the State agency regarding the initial
18 planning of an information technology project, the
19 content and design of a request for proposals, contract
20 development, procurement and architectural and other
21 technical reviews.
22 (ii) Monitor progress in the development and
23 implementation of an information technology project.
24 (iii) Provide status reports to the State agency and
25 the director, including recommendations regarding
26 continued approval of an information technology project.
27 (3) Personnel of the State agency to which a project
28 management assistant is designated shall provide periodic
29 reports to the project management assistant regarding an
30 information technology project. Each report shall include
31 information regarding the following:
32 (i) The State agency's business requirements.
33 (ii) Applicable laws and regulations.
34 (iii) Project costs.
35 (iv) Issues related to hardware, software or
36 training.
37 (v) Projected and actual completion dates for the
38 project.
39 (vi) Any other information related to the
40 implementation of the project.
41 § 4335. Dispute resolution.
42 (a) Right to request for review.--If the director has
43 disapproved or suspended an information technology project or
44 has disapproved a State agency's request for an amended version
45 of the plan for the project, the affected State agency may
46 request the director to revisit the determination about the
47 project. The request for review shall be submitted in writing to
48 the director within 15 business days following the State
49 agency's receipt of the disapproval or suspension.
50 (b) Contents of request for review.--A request for review
51 under subsection (a) shall specify the grounds for the State

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

4 (c) Notification.--

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

9 (2) If the director approves the implementation of a
10 modified project by a State agency, the director shall notify
11 the State Treasurer and the Secretary of the Budget
12 immediately. The State agency shall notify all contracted
13 third parties of any changes or modifications to the project.
14 § 4336. Purchase of certain equipment prohibited.

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

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

28 § 4337. Refurbished computer equipment purchasing program.

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

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

39 (1) The director.

40 (2) The General Assembly.

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

44 § 4338. Data on reliability and other matters.

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

49 (b) Report.--The office shall transmit a report regarding
50 the matters under subsection (a) by February 1, 2020, and
51 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

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

3 § 4346. Confidentiality.

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

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

11 § 4347. Methods of procurement.

12 (a) Electronic procurement.--

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

16 (2) The following shall apply regarding reverse
17 auctions:

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

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

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

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

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

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

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

42 (b) Bulk purchasing.--

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

46 (i) The aggregation of hardware purchases.

47 (ii) The use of formal bid procedures.

48 (iii) Restrictions on supplemental staffing.

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

51 (v) Information technology as a service.

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

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

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

14 (1) The best value of the purchase.

15 (2) Compliance with information technology project
16 management policies.

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

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

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

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

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

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

33 (1) The Secretary of the Budget.

34 (2) The Auditor General.

35 (3) The General Assembly.

36 § 4348. Quality assurance.

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

40 SUBCHAPTER E

41 SECURITY

42 Sec.

43 4351. Statewide security standards.

44 4352. Security standards and risk assessments.

45 4353. Assessment of compliance with security standards.

46 4354. Joint Cybersecurity Oversight Committee.

47 § 4351. Statewide security standards.

48 (a) Establishment.--

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

1 Commonwealth's distributed information technology assets,
2 including:

- 3 (i) Data classification.
- 4 (ii) Management.
- 5 (iii) Communications.
- 6 (iv) Encryption technologies.

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

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

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

20 § 4352. Security standards and risk assessments.

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

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

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

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

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

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

- 49 (i) Identity management.
- 50 (ii) Security incident management.
- 51 (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

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

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

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

10 § 4354. Joint Cybersecurity Oversight Committee.

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

14 (1) The director.

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

17 (i) Two members of the Senate.

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

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

22 (i) One member of the Senate.

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

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

27 (i) Two members of the House of Representatives.

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

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

33 (i) One member of the House of Representatives.

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

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

39 (7) The chief information officer of:

40 (i) The Department of the Auditor General.

41 (ii) The Treasury Department.

42 (iii) The Office of Attorney General.

43 (iv) The Administrative Office of Pennsylvania
44 Courts.

45 (v) The Pennsylvania Public Utility Commission.

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

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

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

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

5 (c) Staffing.--

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

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

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

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

16 (f) Meetings.--

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

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

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

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

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

34 (6) A meeting of the committee shall not be subject to
35 65 Pa.C.S. Ch. 7 (relating to open meetings).

36 (7) A meeting held by the Committee in which the
37 committee accepts testimony shall comply with 65 Pa.C.S. Ch.
38 7.

39 (g) Duties.--

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

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

46 (i) The Governor.

47 (ii) The President pro tempore of the Senate.

48 (iii) The Speaker of the House of Representatives.

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

51 (v) The Majority Leader and the Minority Leader of

1 the House of Representatives.

2 (vi) The Court Administrator of Pennsylvania.

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

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

8 SUBCHAPTER F

9 ENFORCEMENT AND PENALTIES

10 Sec.

11 4361. Administrative and judicial review.

12 4362. Unauthorized use for private benefit prohibited.

13 4363. Financial interests.

14 4364. Certification of submittal without collusion.

15 § 4361. Administrative and judicial review.

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

19 § 4362. Unauthorized use for private benefit prohibited.

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

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

29 § 4363. Financial interests.

30 (a) Offense.--

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

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

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

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

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

1 § 4364. Certification of submittal without collusion.

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

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

8 Subchapter G

9 Pennsylvania Statewide Radio Network

10 Sec.

11 4371. Definitions.

12 4372. Administration of PA-STARNet.

13 4373. PA-STARNet Committee.

14 § 4371. Definitions.

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

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

23 "Commissioner." The Commissioner of Pennsylvania State
24 Police.

25 "Committee." The PA-STARNet Committee established under §
26 4373 (relating to PA-STARNet Committee).

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

30 "First responder." An individual who in the early stages of
31 an incident is responsible for the protection and preservation
32 of life, property, evidence and the environment, including
33 emergency response providers as that term is defined in section
34 2 of the Homeland Security Act of 2002 (Public Law 107-296, 116
35 Stat. 2135).

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

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

49 "Public safety communications." The means and methods for
50 transmitting and receiving information necessary for the conduct
51 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.