
THE GENERAL ASSEMBLY OF PENNSYLVANIA

HOUSE BILL

No. 2567 Session of
2020

INTRODUCED BY GROVE, JUNE 8, 2020

REFERRED TO COMMITTEE ON STATE GOVERNMENT, JUNE 8, 2020

AN ACT

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

10 The General Assembly of the Commonwealth of Pennsylvania
11 hereby enacts as follows:

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

14 CHAPTER 43

15 INFORMATION TECHNOLOGY

16 Subchapter

17 A. General Provisions

18 B. Office of Information Technology

19 C. Business Operations

20 D. Procurement of Information Technology

21 E. Security

22 F. Enforcement and Penalties

1 G. Pennsylvania Statewide Radio Network

2 SUBCHAPTER A

3 GENERAL PROVISIONS

4 Sec.

5 4301. Scope of chapter.

6 4302. Findings and declarations.

7 4303. Definitions.

8 § 4301. Scope of chapter.

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

11 § 4302. Findings and declarations.

12 The General Assembly finds and declares the following:

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

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

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

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

28 (5) By reforming the Commonwealth's outdated approach to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

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

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

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

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

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

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

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

23 § 4303. Definitions.

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

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

30 "Authorization to operate." A formal declaration by the head

1 of the State agency that:

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

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

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

13 (1) The State's current technology.

14 (2) The opportunities for technology sharing.

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

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

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

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

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

30 "Independent agency." As follows:

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

4 (2) The term does not include:

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

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

9 "Independent department." Any of the following:

10 (1) The Department of the Auditor General.

11 (2) The Treasury Department.

12 (3) The Office of Attorney General.

13 (4) A board or commission of an entity under paragraph
14 (1), (2) or (3).

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

18 (1) Personal computers.

19 (2) Servers.

20 (3) Mainframes.

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

22 (5) Broadband.

23 (6) Mobile or portable computers.

24 (7) Peripheral equipment.

25 (8) Telephones.

26 (9) Wireless communications.

27 (10) Handheld devices.

28 (11) Facsimile machines.

29 (12) Technology facilities, including, but not limited
30 to, data centers, dedicated training facilities or switching

1 facilities.

2 (13) Electronic payment processing services.

3 (14) Other relevant hardware and software items or
4 personnel tasked with the planning, implementation or support
5 of technology, including hosting or vendor-managed service
6 solutions.

7 "Information technology budget." As follows:

8 (1) All information technology expenditures listed by
9 project and amount of expenditure for planning, development,
10 modernization, operations and maintenance.

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

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

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

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

27 "Portal." A publicly available Internet website.

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

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

3 "State agency." Any of the following:

4 (1) The Governor's Office.

5 (2) A department, board, commission, authority or other
6 agency of the Commonwealth that is subject to the policy
7 supervision and control of the Governor.

8 (3) The office of Lieutenant Governor.

9 (4) An independent agency.

10 SUBCHAPTER B

11 OFFICE OF INFORMATION TECHNOLOGY

12 Sec.

13 4311. Establishment of office.

14 4312. Duties of office.

15 4313. Director.

16 4314. Transfer of additional duties and personnel.

17 4315. Planning and financing information technology resources.

18 4316. Commonwealth Information Technology Fund.

19 4317. Financial accountability and information technology.

20 4318. Commonwealth portal.

21 4319. Statewide information technology transparency portal.

22 4320. State agency requests for information technology and
23 services.

24 4321. Status of information technology projects and corrective
25 action plans.

26 § 4311. Establishment of office.

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

1 § 4312. Duties of office.

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

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

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

10 (i) The development of priorities and strategic
11 plans.

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

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

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

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

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

- 1 (i) Defining an information technology strategy
2 plan.
- 3 (ii) Defining enterprise architecture.
- 4 (iii) Determining technological direction.
- 5 (iv) Defining information technology organization
6 and relationships.
- 7 (v) Managing information technology investment.
- 8 (vi) Communicating management aims and direction.
- 9 (vii) Managing information technology human
10 resources.
- 11 (viii) Managing quality.
- 12 (ix) Assessing risks.
- 13 (x) Managing projects.
- 14 (xi) Identifying automated solutions.
- 15 (xii) Acquiring and maintaining application
16 software.
- 17 (xiii) Acquiring and maintaining technology
18 infrastructure.
- 19 (xiv) Enabling operation and use.
- 20 (xv) Procuring information technology resources.
- 21 (xvi) Managing changes.
- 22 (xvii) Installing and accrediting solutions and
23 changes.
- 24 (xviii) Defining and managing service levels.
- 25 (xix) Managing third-party services.
- 26 (xx) Managing performance and capacity.
- 27 (xxi) Ensuring continuous service.
- 28 (xxii) Ensuring system security.
- 29 (xxiii) Identifying and allocating costs.
- 30 (xxiv) Educating and training users.

1 (xxv) Managing service desk and incidents.

2 (xxvi) Managing the configuration.

3 (xxvii) Managing problems.

4 (xxviii) Managing data.

5 (xxix) Managing physical environment.

6 (xxx) Managing operations.

7 (xxxi) Monitoring and evaluating information
8 technology performance.

9 (xxxii) Monitoring and evaluating internal controls.

10 (xxxiii) Ensuring compliance with external
11 requirements.

12 (xxxiv) Providing improved information technology
13 governance.

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

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

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

22 (3) Establish information technology security standards.

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

25 (5) Develop a schedule for the replacement or
26 modification of information technology systems.

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

30 (7) Prescribe the manner of inspecting or testing

1 information technology assets, systems or personnel to
2 determine compliance with information technology plans,
3 specifications and requirements.

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

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

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

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

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

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

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

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

29 (16) Ensure the proper use of project management
30 methodologies and principles on information technology

1 projects, including measures to review project delivery and
2 quality.

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

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

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

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

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

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

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

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

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

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

28 (23) Establish and operate centers of expertise for
29 specific information technologies and services to serve two
30 or more State agencies on a cost-sharing basis, if the

1 director, after consultation with the Office of the Budget,
2 decides it is advisable from the standpoint of the
3 information technology strategic plan, efficiency and economy
4 to establish these centers and services.

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

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

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

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

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

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

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

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

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

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

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

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

12 (36) Establish a process for the following:

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

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

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

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

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

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

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

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

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

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

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

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

26 (47) Develop and facilitate data sharing and data
27 analytics to minimize redundancy and align information
28 technology spending in a manner that reduces costs and
29 measurably improves Commonwealth agency mission
30 effectiveness.

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

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

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

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

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

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

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

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

24 § 4313. Director.

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

27 (b) Qualifications.--The director must be qualified by
28 experience for the office and have at least five years of
29 experience dealing with public sector information systems in a
30 State government agency or an equivalent entity. The

1 qualifications shall include, but are not limited to, verifying
2 that an individual has the proper industry certifications
3 necessary to perform the duties under this chapter.

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

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

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

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

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

18 (5) Notify the Treasury Department in order to suspend
19 funding for a program that has been designated as the color
20 red in accordance with section 4321 (relating to status of
21 information technology projects and corrective action plans).

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

26 (e) Disaster recovery plan.--

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

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

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

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

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

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

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

18 § 4314. Transfer of additional duties and personnel.

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

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

26 (i) Report directly to the director.

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

30 (2) An employee of a State agency who handles or

1 otherwise has responsibility for the State agency's
2 information technology services shall be transferred to the
3 office and operate in the physical location of the State
4 agency or the shared services center supporting that agency,
5 but the employee shall report matters to the office and be
6 supervised by the chief information officer of the State
7 agency or head of the shared services center.

8 (3) The chief information officer of each agency or
9 shared service center shall be responsible for identifying
10 and implementing actions and milestones as required to
11 fulfill the remediation plan determined by the director under
12 section 4313(c)(4) (relating to director).

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

17 § 4315. Planning and financing information technology
18 resources.

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

23 (b) Development of plan.--

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

30 (i) The plan may include current applications and

1 infrastructure, migration from current environments and
2 other information necessary for fiscal or technology
3 planning.

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

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

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

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

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

19 (c) Consultation and cooperation.--

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

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

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

1 technology assets, including resources provided by the State
2 agency or through contracts or grants.

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

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

7 (d) Biennial plan.--

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

12 (2) The biennial plan shall include:

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

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

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

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

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

28 § 4316. Commonwealth Information Technology Fund.

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

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

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

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

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

12 (c) Use of fund money.--

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

16 (i) Project management.

17 (ii) Security.

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

20 (iv) State portal operations.

21 (v) State agencies' annual information technology
22 budget.

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

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

29 § 4317. Financial accountability and information technology.

30 (a) Development of processes.--Subject to subsection (b),

1 the office, along with the Secretary of the Budget and the State
2 Treasurer, shall develop processes for budgeting and accounting
3 of expenditures for information technology operations, including
4 all Commonwealth personnel, services, projects, infrastructure
5 and assets across all State agencies.

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

9 (1) Hardware.

10 (2) Software.

11 (3) Personnel.

12 (4) Training.

13 (5) Contractual services, including cloud service
14 providers.

15 (6) Other items relevant to information technology.

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

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

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

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

27 (3) The total appropriation for each service.

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

30 (5) Any other use of State data by the vendor and the

1 total amount of revenue collected per use and in total.

2 (6) User satisfaction with each service.

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

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

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

10 (2) Line-item details on expenditures.

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

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

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

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

18 (1) The Secretary of the Budget.

19 (2) The Independent Fiscal Office.

20 § 4318. Commonwealth portal.

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

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

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

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

4 § 4319. Statewide information technology transparency portal.

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

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

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

16 (2) The approved budget of each project.

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

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

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

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

30 (i) If an information technology project has not

1 exceeded the completion date in the original contract,
2 the project shall be designated as the color green.

3 (ii) If an information technology project has
4 exceeded the completion date in the original contract,
5 the project shall be designated as the color red.

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

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

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

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

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

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

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

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

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

1 § 4320. State agency requests for information technology and
2 services.

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

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

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

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

26 (i) Organization, process and technology options.

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

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

4 § 4321. Status of information technology projects and
5 corrective action plans.

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

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

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

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

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

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

30 (c) Additional requirements.--The director shall notify the

1 State Treasurer to suspend future expenditure of funds for any
2 technology project that is designated as red under this section
3 and that fails to adopt a remediation plan within the time
4 outlined under this section. The following shall apply:

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

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

16 SUBCHAPTER C

17 BUSINESS OPERATIONS

18 Sec.

19 4331. Reporting requirements regarding procurement.

20 4332. Communications services.

21 4333. Project approval standards.

22 4334. Project management standards.

23 4335. Dispute resolution.

24 4336. Purchase of certain equipment prohibited.

25 4337. Refurbished computer equipment purchasing program.

26 4338. Data on reliability and other matters.

27 § 4331. Reporting requirements regarding procurement.

28 (a) Bids.--A vendor submitting a bid or proposal shall
29 disclose in a statement, provided contemporaneously with the bid
30 or proposal, where services will be performed under the contract

1 sought, including any subcontracts, and whether any services
2 under that contract, including any subcontracts, are anticipated
3 to be performed outside the United States.

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

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

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

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

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

16 § 4332. Communications services.

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

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

28 (2) Provide for the establishment, management and
29 operation, through State ownership, by contract or through
30 commercial leasing, of the following systems and services as

1 they affect the internal management and operation of State
2 agencies:

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

6 (ii) Satellite services.

7 (iii) Closed-circuit television systems.

8 (iv) Two-way radio systems.

9 (v) Microwave systems.

10 (vi) Related systems based on telecommunication
11 technologies.

12 (vii) Broadband.

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

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

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

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

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

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

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

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

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

21 § 4333. Project approval standards.

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

27 (1) the project conforms to project management
28 procedures and policies and to procurement rules and
29 policies; and

30 (2) sufficient funds are available for implementation.

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

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

- 9 (1) The State agency.
- 10 (2) The Secretary of the Budget.
- 11 (3) The State Treasurer.
- 12 (4) The Auditor General.
- 13 (5) The General Assembly.

14 (d) Suspension.--

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

- 17 (i) fails to meet the applicable quality assurance
18 standards;
- 19 (ii) has exceeded its projected costs; or
- 20 (iii) has failed to meet its projected completion
21 date.

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

- 28 (i) The State agency.
- 29 (ii) The Secretary of the Budget.
- 30 (iii) The State Treasurer.

1 (iv) The Auditor General.

2 (v) The General Assembly.

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

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

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

18 (i) The director.

19 (ii) The Governor.

20 (iii) The Secretary of the Budget.

21 (iv) The General Assembly.

22 § 4334. Project management standards.

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

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

30 (c) Project management assistant.--

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

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

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

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

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

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

21 (i) The State agency's business requirements.

22 (ii) Applicable laws and regulations.

23 (iii) Project costs.

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

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

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

30 § 4335. Dispute resolution.

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

9 (b) Contents of request for review.--A request for review
10 under subsection (a) shall specify the grounds for the State
11 agency's disagreement with the director's determination. The
12 State agency shall include with its request a plan to modify the
13 project to meet the director's concerns.

14 (c) Notification.--

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

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

24 § 4336. Purchase of certain equipment prohibited.

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

1 televisions.

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

8 § 4337. Refurbished computer equipment purchasing program.

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

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

19 (1) The director.

20 (2) The General Assembly.

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

24 § 4338. Data on reliability and other matters.

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

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

1 quarterly thereafter to:

2 (1) The Secretary of the Budget.

3 (2) The Independent Fiscal Office.

4 (3) The General Assembly.

5 SUBCHAPTER D

6 PROCUREMENT OF INFORMATION TECHNOLOGY

7 Sec.

8 4345. Duties of office.

9 4346. Confidentiality.

10 4347. Methods of procurement.

11 4348. Quality assurance.

12 § 4345. Duties of office.

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

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

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

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

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

30 (5) Provide strategic sourcing resources and planning to

1 compile and consolidate all estimates of information
2 technology goods and services needed and required by State
3 agencies.

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

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

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

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

20 (b) Specific duties of State agencies.--Subject to the
21 provisions of this chapter and consistent with the processes
22 enacted under 62 Pa.C.S. Ch. 5, each State agency shall have the
23 authority and responsibility to issue purchase orders under
24 contracts entered by the office.

25 § 4346. Confidentiality.

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

29 (b) Proprietary information.--Trade secrets, test data and
30 similar proprietary information and security information

1 protected from disclosure under Federal or State law shall
2 remain confidential.

3 § 4347. Methods of procurement.

4 (a) Electronic procurement.--

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

8 (2) The following shall apply regarding reverse
9 auctions:

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

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

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

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

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

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

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

4 (b) Bulk purchasing.--

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

8 (i) The aggregation of hardware purchases.

9 (ii) The use of formal bid procedures.

10 (iii) Restrictions on supplemental staffing.

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

13 (v) Information technology as a service.

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

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

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

27 (1) The best value of the purchase.

28 (2) Compliance with information technology project
29 management policies.

30 (3) Compliance with information technology security

1 standards and policies.

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

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

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

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

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

16 (1) The Secretary of the Budget.

17 (2) The Auditor General.

18 (3) The General Assembly.

19 § 4348. Quality assurance.

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

23 SUBCHAPTER E

24 SECURITY

25 Sec.

26 4351. Statewide security standards.

27 4352. Security standards and risk assessments.

28 4353. Assessment of compliance with security standards.

29 4354. Joint Cybersecurity Oversight Committee.

30 § 4351. Statewide security standards.

1 (a) Establishment.--

2 (1) The director shall establish a Statewide set of
3 standards for information technology security to maximize the
4 functionality, security and interoperability of the
5 Commonwealth's distributed information technology assets,
6 including:

7 (i) Data classification.

8 (ii) Management.

9 (iii) Communications.

10 (iv) Encryption technologies.

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

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

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

24 § 4352. Security standards and risk assessments.

25 (a) Authorization to operate.--Notwithstanding any other
26 provision of law and except as otherwise provided by this
27 chapter, all information technology security goods, software or
28 services purchased using taxpayer money, or for use by a State
29 agency or in a public facility, shall require an authorization
30 to operate by the head of the State agency in accordance with

1 security standards under this chapter. No information technology
2 system or service may be operated by, or in support of, a State
3 agency without an authorization to operate.

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

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

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

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

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

23 (i) Identity management.

24 (ii) Security incident management.

25 (iii) Network perimeter security.

26 (iv) Systems development.

27 (v) Project management.

28 (vi) Information technology risk management.

29 (vii) Data management.

30 (viii) Vulnerability management.

1 (4) Detailed reports of the risk and security issues
2 identified in the assessments shall be reported to the
3 director and shall be kept confidential.

4 (5) The agency head, in consultation with the office,
5 shall identify corrective or mitigating actions as needed.

6 (d) Interim authority to operate.--If the agency head
7 determines that the information technology system or service is
8 needed, the agency head may seek authorization from the director
9 for a period not longer than 180 days to implement the
10 corrective or mitigating actions.

11 (e) Security audit.--

12 (1) The director shall contract with an independent
13 certified information security auditor or entity to perform
14 an information security audit of State agencies.

15 (2) The director shall determine a schedule for
16 continuous State agency information security audits.

17 (f) Notification and audits.--The following shall apply:

18 (1) The party conducting the assessment or audit shall
19 provide the director and head of the reviewed State agency
20 with a detailed report of the security issues identified,
21 which shall not be publicly disclosed.

22 (2) The State agency, in cooperation with the office,
23 shall provide the director with a corrective action plan that
24 remediates issues identified in the detailed report under
25 paragraph (1), which shall not be publicly disclosed.

26 (3) The director shall issue a public report on the
27 general results of the assessment that shall be accessible on
28 the portal under section 4319 (relating to Statewide
29 information technology transparency portal).

30 (g) Effect of section.--Nothing in this section shall be

1 construed to preclude the Auditor General or the General
2 Assembly from assessing the security practices of State
3 information technology systems as part of its statutory duties
4 and responsibilities.

5 § 4353. Assessment of compliance with security standards.

6 (a) Frequency.--The director shall biannually assess the
7 ability of each State agency's contracted vendors to comply with
8 the current security standards established under this chapter.

9 (b) Contents.--The director shall establish a quantifiable
10 objective metric that measures the degree of compliance with
11 current security standards. The assessment under this section
12 shall, at a minimum:

13 (1) Quantify the degree of compliance with the current
14 security standards using the metric.

15 (2) Include security organization, security practices,
16 security information standards, network security
17 architecture, systems development and lifecycle management
18 and current expenditures of State funds for information
19 security.

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

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

26 § 4354. Joint Cybersecurity Oversight Committee.

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

30 (1) The director.

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

3 (i) Two members of the Senate.

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

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

8 (i) One member of the Senate.

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

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

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

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

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

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

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

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

25 (7) The chief information officer of:

26 (i) The Department of the Auditor General.

27 (ii) The Treasury Department.

28 (iii) The Office of Attorney General.

29 (iv) The Administrative Office of Pennsylvania
30 Courts.

1 (v) The Pennsylvania Public Utility Commission.

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

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

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

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

12 (c) Staffing.--

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

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

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

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

23 (f) Meetings.--

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

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

29 (3) The chairperson of the committee shall provide the
30 members of the committee with notice of the time and location

1 of each meeting of the committee no later than one week prior
2 to the meeting. Notice shall also be provided to the
3 Governor, the President pro tempore of the Senate and the
4 Speaker of the House of Representatives.

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

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

11 (6) A meeting of the committee shall not be subject to
12 65 Pa.C.S. Ch. 7 (relating to open meetings).

13 (7) A meeting held by the Committee in which the
14 committee accepts testimony shall comply with 65 Pa.C.S. Ch.
15 7.

16 (g) Duties.--

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

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

23 (i) The Governor.

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

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

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

28 (v) The Majority Leader and the Minority Leader of
29 the House of Representatives.

30 (vi) The Court Administrator of Pennsylvania.

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

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

6 SUBCHAPTER F

7 ENFORCEMENT AND PENALTIES

8 Sec.

9 4361. Administrative and judicial review.

10 4362. Unauthorized use for private benefit prohibited.

11 4363. Financial interests.

12 4364. Certification of submittal without collusion.

13 § 4361. Administrative and judicial review.

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

17 § 4362. Unauthorized use for private benefit prohibited.

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

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

27 § 4363. Financial interests.

28 (a) Offense.--

29 (1) The director, any other policymaking employee of the
30 office and any employee of a State agency involved in

1 management or oversight, including contract administration,
2 of the information technology project may not have a
3 financial interest or personal beneficial interest, either
4 directly or indirectly, in the purchase of or contract for
5 information technology. The financial interest or personal
6 interest shall extend to a corporation, partnership, company,
7 trust, association or other entity furnishing information
8 technology to the Commonwealth or any of its State agencies.

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

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

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

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

20 § 4364. Certification of submittal without collusion.

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

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

27 Subchapter G

28 Pennsylvania Statewide Radio Network

29 Sec.

30 4371. Definitions.

1 4372. Administration of PA-STARNet.

2 4373. PA-STARNet Committee.

3 § 4371. Definitions.

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

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

12 "Commissioner." The Commissioner of Pennsylvania State
13 Police.

14 "Committee." The PA-STARNet Committee established under §
15 4373 (relating to PA-STARNet Committee).

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

19 "First responder." An individual who in the early stages of
20 an incident is responsible for the protection and preservation
21 of life, property, evidence and the environment, including
22 emergency response providers as that term is defined in section
23 2 of the Homeland Security Act of 2002 (Public Law 107-296, 116
24 Stat. 2135).

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

28 "Pennsylvania Statewide Radio Network" or "PA-STARNet." A
29 Statewide radio network comprising a communication and
30 information infrastructure connected by a digital microwave

1 system for transmission of voice and data, including all
2 frequency bands and other system extensions owned and operated
3 by the Commonwealth and connected to the core digital trunked
4 radio network operating in the 800 megahertz (MHz) public safety
5 frequency band and in other public safety frequency bands
6 licensed by the Federal Communications Commission (FCC), or to
7 the microwave backbone network.

8 "Public safety communications." The means and methods for
9 transmitting and receiving information necessary for the conduct
10 of services rendered by or through Federal, State or local
11 government entities in support of the protection and
12 preservation of life, property and natural resources, as
13 prescribed by law.

14 "State police." The Pennsylvania State Police.
15 § 4372. Administration of PA-STARNet.

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

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

22 (1) the benefit of the participating agencies;
23 (2) the support of effective communications at critical
24 public events; and

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

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

1 § 4373. PA-STARNet Committee.

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

8 Section 2. This act shall take effect immediately.