
THE GENERAL ASSEMBLY OF PENNSYLVANIA

SENATE BILL

No. 284 Session of
2023

INTRODUCED BY PHILLIPS-HILL, AUMENT, DUSH, MARTIN, STEFANO,
J. WARD, LAUGHLIN, ROTHMAN, BAKER, VOGEL AND REGAN,
JANUARY 31, 2023

REFERRED TO COMMUNICATIONS AND TECHNOLOGY, JANUARY 31, 2023

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

1 F. Enforcement and Penalties

2 G. Pennsylvania Statewide Radio Network

3 SUBCHAPTER A

4 GENERAL PROVISIONS

5 Sec.

6 4301. Scope of chapter.

7 4302. Findings and declarations.

8 4303. Definitions.

9 § 4301. Scope of chapter.

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

12 § 4302. Findings and declarations.

13 The General Assembly finds and declares as follows:

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

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

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

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

29 (5) By reforming the Commonwealth's outdated approach to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

1 analytic capabilities and improve cybersecurity.

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

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

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

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

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

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

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

24 § 4303. Definitions.

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

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

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

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

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

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

14 (1) The State's current technology.

15 (2) The opportunities for technology sharing.

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

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

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

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

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

1 "Independent agency." As follows:

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

5 (2) The term does not include:

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

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

10 "Independent department." Any of the following:

11 (1) The Department of the Auditor General.

12 (2) The Treasury Department.

13 (3) The Office of Attorney General.

14 (4) A board or commission of an entity under paragraph
15 (1), (2) or (3).

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

19 (1) Personal computers.

20 (2) Servers.

21 (3) Mainframes.

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

23 (5) Broadband.

24 (6) Mobile or portable computers.

25 (7) Peripheral equipment.

26 (8) Telephones.

27 (9) Wireless communications.

28 (10) Handheld devices.

29 (11) Facsimile machines.

30 (12) Technology facilities, including, but not limited

1 to, data centers, dedicated training facilities or switching
2 facilities.

3 (13) Electronic payment processing services.

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

8 "Information technology budget." As follows:

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

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

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

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

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

28 "Portal." A publicly available Internet website.

29 "Reverse auction." A real-time purchasing process in which
30 vendors compete to provide goods or services at the lowest

1 selling price in an open and interactive electronic environment.

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

4 "State agency." Any of the following:

5 (1) The Governor's Office.

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

9 (3) The office of Lieutenant Governor.

10 (4) An independent agency.

11 SUBCHAPTER B

12 OFFICE OF INFORMATION TECHNOLOGY

13 Sec.

14 4311. Establishment of office.

15 4312. Duties of office.

16 4313. Director.

17 4314. Transfer of additional duties and personnel.

18 4315. Planning and financing information technology resources.

19 4316. Commonwealth Information Technology Fund.

20 4317. Financial accountability and information technology.

21 4318. Commonwealth portal.

22 4319. Statewide information technology transparency portal.

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

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

27 § 4311. Establishment of office.

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

1 chapter.

2 § 4312. Duties of office.

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

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

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

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

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

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

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

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

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

1 include:

2 (i) Defining an information technology strategy
3 plan.

4 (ii) Defining enterprise architecture.

5 (iii) Determining technological direction.

6 (iv) Defining information technology organization
7 and relationships.

8 (v) Managing information technology investment.

9 (vi) Communicating management aims and direction.

10 (vii) Managing information technology human
11 resources.

12 (viii) Managing quality.

13 (ix) Assessing risks.

14 (x) Managing projects.

15 (xi) Identifying automated solutions.

16 (xii) Acquiring and maintaining application
17 software.

18 (xiii) Acquiring and maintaining technology
19 infrastructure.

20 (xiv) Enabling operation and use.

21 (xv) Procuring information technology resources.

22 (xvi) Managing changes.

23 (xvii) Installing and accrediting solutions and
24 changes.

25 (xviii) Defining and managing service levels.

26 (xix) Managing third-party services.

27 (xx) Managing performance and capacity.

28 (xxi) Ensuring continuous service.

29 (xxii) Ensuring system security.

30 (xxiii) Identifying and allocating costs.

- 1 (xxiv) Educating and training users.
- 2 (xxv) Managing service desk and incidents.
- 3 (xxvi) Managing the configuration.
- 4 (xxvii) Managing problems.
- 5 (xxviii) Managing data.
- 6 (xxix) Managing physical environment.
- 7 (xxx) Managing operations.
- 8 (xxxi) Monitoring and evaluating information
9 technology performance.
- 10 (xxxii) Monitoring and evaluating internal controls.
- 11 (xxxiii) Ensuring compliance with external
12 requirements.
- 13 (xxxiv) Providing improved information technology
14 governance.

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

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

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

23 (3) Establish information technology security standards.

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

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

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

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

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

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

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

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

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

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

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

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

30 (16) Ensure the proper use of project management

1 methodologies and principles on information technology
2 projects, including measures to review project delivery and
3 quality.

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

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

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

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

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

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

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

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

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

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

29 (23) Establish and operate centers of expertise for
30 specific information technologies and services to serve two

1 or more State agencies on a cost-sharing basis, if the
2 director, after consultation with the Office of the Budget,
3 decides it is advisable from the standpoint of the
4 information technology strategic plan, efficiency and economy
5 to establish these centers and services.

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

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

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

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

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

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

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

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

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

1 and investment and review processes.

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

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

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

13 (36) Establish a process for the following:

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

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

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

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

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

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

1 necessary.

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

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

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

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

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

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

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

1 effectiveness.

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

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

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

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

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

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

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

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

25 § 4313. Director.

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

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

1 State government agency or an equivalent entity. The
2 qualifications shall include, but are not limited to, verifying
3 that an individual has the proper industry certifications
4 necessary to perform the duties under this chapter.

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

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

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

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

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

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

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

27 (e) Disaster recovery plan.--

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

1 implement the plan.

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

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

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

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

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

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

19 § 4314. Transfer of additional duties and personnel.

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

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

27 (i) Report directly to the director.

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

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

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

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

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

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

24 (b) Development of plan.--

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

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

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

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

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

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

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

20 (c) Consultation and cooperation.--

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

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

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

1 to determine full costs and expenditures for information
2 technology assets, including resources provided by the State
3 agency or through contracts or grants.

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

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

8 (d) Biennial plan.--

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

13 (2) The biennial plan shall include:

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

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

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

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

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

29 § 4316. Commonwealth Information Technology Fund.

30 (a) Establishment.--An account is established in the General

1 Fund to be known as the Information Technology Fund.

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

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

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

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

13 (c) Use of fund money.--

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

17 (i) Project management.

18 (ii) Security.

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

21 (iv) State portal operations.

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

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

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

30 § 4317. Financial accountability and information technology.

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

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

10 (1) Hardware.

11 (2) Software.

12 (3) Personnel.

13 (4) Training.

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

16 (6) Other items relevant to information technology.

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

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

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

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

28 (3) The total appropriation for each service.

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

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

3 (6) User satisfaction with each service.

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

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

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

11 (2) Line-item details on expenditures.

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

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

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

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

19 (1) The Secretary of the Budget.

20 (2) The Independent Fiscal Office.

21 § 4318. Commonwealth portal.

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

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

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

1 government.

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

5 § 4319. Statewide information technology transparency portal.

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

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

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

17 (2) The approved budget of each project.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

30 (2) The policy intranet documents shall be made

1 available via the web-based portal when deployed.
2 § 4320. State agency requests for information technology and
3 services.

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

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

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

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

27 (i) Organization, process and technology options.

28 (ii) At least three alternatives, including the
29 status quo, a shared service or external service option
30 and any other alternatives consistent with the

1 architecture and strategy developed by the office.

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

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

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

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

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

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

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

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

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

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

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

17 SUBCHAPTER C

18 BUSINESS OPERATIONS

19 Sec.

20 4331. Reporting requirements regarding procurement.

21 4332. Communications services.

22 4333. Project approval standards.

23 4334. Project management standards.

24 4335. Dispute resolution.

25 4336. Purchase of certain equipment prohibited.

26 4337. Refurbished computer equipment purchasing program.

27 4338. Data on reliability and other matters.

28 § 4331. Reporting requirements regarding procurement.

29 (a) Bids.--A vendor submitting a bid or proposal shall
30 disclose in a statement, provided contemporaneously with the bid

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

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

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

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

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

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

17 § 4332. Communications services.

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

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

29 (2) Provide for the establishment, management and
30 operation, through State ownership, by contract or through

1 commercial leasing, of the following systems and services as
2 they affect the internal management and operation of State
3 agencies:

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

7 (ii) Satellite services.

8 (iii) Closed-circuit television systems.

9 (iv) Two-way radio systems.

10 (v) Microwave systems.

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

13 (vii) Broadband.

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

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

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

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

29 (7) Provide every three years an inventory of
30 telecommunications costs, facilities, systems and personnel

1 within State agencies.

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

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

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

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

22 § 4333. Project approval standards.

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

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

1 (2) sufficient funds are available for implementation.

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

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

10 (1) The State agency.

11 (2) The Secretary of the Budget.

12 (3) The State Treasurer.

13 (4) The Auditor General.

14 (5) The General Assembly.

15 (d) Suspension.--

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

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

20 (ii) has exceeded its projected costs; or

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

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

29 (i) The State agency.

30 (ii) The Secretary of the Budget.

1 (iii) The State Treasurer.

2 (iv) The Auditor General.

3 (v) The General Assembly.

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

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

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

19 (i) The director.

20 (ii) The Governor.

21 (iii) The Secretary of the Budget.

22 (iv) The General Assembly.

23 § 4334. Project management standards.

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

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

1 (c) Project management assistant.--

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

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

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

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

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

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

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

23 (ii) Applicable laws and regulations.

24 (iii) Project costs.

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

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

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

1 § 4335. Dispute resolution.

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

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

15 (c) Notification.--

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

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

25 § 4336. Purchase of certain equipment prohibited.

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

1 the procurement of information technology equipment and
2 televisions.

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

9 § 4337. Refurbished computer equipment purchasing program.

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

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

20 (1) The director.

21 (2) The General Assembly.

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

25 § 4338. Data on reliability and other matters.

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

30 (b) Report.--The office shall transmit a report regarding

1 the matters under subsection (a) by February 1, 2021, and
2 quarterly thereafter to:

3 (1) The Secretary of the Budget.

4 (2) The Independent Fiscal Office.

5 (3) The General Assembly.

6 SUBCHAPTER D

7 PROCUREMENT OF INFORMATION TECHNOLOGY

8 Sec.

9 4345. Duties of office.

10 4346. Confidentiality.

11 4347. Methods of procurement.

12 4348. Quality assurance.

13 § 4345. Duties of office.

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

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

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

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

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

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

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

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

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

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

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

26 § 4346. Confidentiality.

27 (a) Contract information.--Subject to subsection (b),
28 contract information compiled by the office shall be made a
29 matter of public record in accordance with 62 Pa.C.S. § 512
30 (relating to competitive sealed bidding).

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

5 § 4347. Methods of procurement.

6 (a) Electronic procurement.--

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

10 (2) The following shall apply regarding reverse
11 auctions:

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

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

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

18 (iv) All requirements relating to formal and
19 competitive bids, including advertisement, seal and
20 signature, are satisfied when a procurement is conducted
21 or a contract is entered in compliance with the reverse
22 auction or electronic bidding requirements established by
23 the office. Advertisement for the reverse auction must be
24 conducted in accordance with 62 Pa.C.S. § 512.1 (relating
25 to competitive electronic auction bidding).

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

29 (vi) The office shall not use reverse auctions for
30 the procurement of information technology services,

1 hardware software or solutions that incorporate both
2 information technology hardware and services, including,
3 but not limited to, cloud-based information technology
4 solutions.

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

8 (b) Bulk purchasing.--

9 (1) The director shall establish procedures for the
10 procurement of information technology through bulk purchases.

11 The procedures may include the following:

12 (i) The aggregation of hardware purchases.

13 (ii) The use of formal bid procedures.

14 (iii) Restrictions on supplemental staffing.

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

17 (v) Information technology as a service.

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

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

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

1 (1) The best value of the purchase.

2 (2) Compliance with information technology project
3 management policies.

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

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

8 (e) Exceptions.--In addition to permitted waivers of
9 competition, the requirements of competitive bidding shall not
10 apply to information technology contracts and procurements in
11 the case of a pressing need or an emergency arising from an
12 information technology security incident.

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

17 (1) The Secretary of the Budget.

18 (2) The Auditor General.

19 (3) The General Assembly.

20 § 4348. Quality assurance.

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

24 SUBCHAPTER E

25 SECURITY

26 Sec.

27 4351. Statewide security standards.

28 4352. Security standards and risk assessments.

29 4353. Assessment of compliance with security standards.

30 4354. Joint Cybersecurity Oversight Committee.

1 § 4351. Statewide security standards.

2 (a) Establishment.--

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

8 (i) Data classification.

9 (ii) Management.

10 (iii) Communications.

11 (iv) Encryption technologies.

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

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

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

25 § 4352. Security standards and risk assessments.

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

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

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

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

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

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

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

24 (i) Identity management.

25 (ii) Security incident management.

26 (iii) Network perimeter security.

27 (iv) Systems development.

28 (v) Project management.

29 (vi) Information technology risk management.

30 (vii) Data management.

1 (viii) Vulnerability management.

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

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

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

12 (e) Security audit.--

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

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

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

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

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

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

1 (g) Effect of section.--Nothing in this section shall be
2 construed to preclude the Auditor General or the General
3 Assembly from assessing the security practices of State
4 information technology systems as part of its statutory duties
5 and responsibilities.

6 § 4353. Assessment of compliance with security standards.

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

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

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

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

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

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

27 § 4354. Joint Cybersecurity Oversight Committee.

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

1 (1) The director.

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

4 (i) Two members of the Senate.

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

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

9 (i) One member of the Senate.

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

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

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

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

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

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

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

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

26 (7) The chief information officer of:

27 (i) The Department of the Auditor General.

28 (ii) The Treasury Department.

29 (iii) The Office of Attorney General.

30 (iv) The Administrative Office of Pennsylvania

1 Courts.

2 (v) The Pennsylvania Public Utility Commission.

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

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

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

9 (11) The president of the County Commissioners
10 Association of Pennsylvania or a designee of the president.

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

15 (c) Staffing.--

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

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

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

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

26 (f) Meetings.--

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

29 (2) The chairperson of the committee, with the consent
30 of the vice chairperson of the committee, may schedule

1 additional meetings of the committee.

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

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

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

14 (6) A meeting of the committee shall be subject to 65
15 Pa.C.S. Ch. 7 (relating to open meetings).

16 (7) Executive sessions may be held in accordance with 65
17 Pa.C.S. § 708 (relating to executive sessions) and may be
18 held to discuss, plan or review matters and records that are
19 deemed necessary for emergency preparedness, protection of
20 public safety and security of all property in a manner that,
21 if disclosed, would be reasonably likely to jeopardize or
22 threaten public safety or preparedness or public protection.

23 (g) Duties.--

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

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

30 (i) The Governor.

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

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

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

5 (v) The Majority Leader and the Minority Leader of
6 the House of Representatives.

7 (vi) The Court Administrator of Pennsylvania.

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

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

13 SUBCHAPTER F

14 ENFORCEMENT AND PENALTIES

15 Sec.

16 4361. Administrative and judicial review.

17 4362. Unauthorized use for private benefit prohibited.

18 4363. Financial interests.

19 4364. Certification of submittal without collusion.

20 § 4361. Administrative and judicial review.

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

24 § 4362. Unauthorized use for private benefit prohibited.

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

29 (b) Criminal penalties and fines.--A person that violates
30 subsection (a) commits a misdemeanor of the first degree. Upon

1 conviction, the person shall be liable to the Commonwealth to
2 repay any amount expended in violation of this chapter, together
3 with any court costs.

4 § 4363. Financial interests.

5 (a) Offense.--

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

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

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

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

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

27 § 4364. Certification of submittal without collusion.

28 (a) Duty.--The director shall require bidders under this
29 chapter to certify that each bid on information technology
30 contracts overseen by the office is submitted competitively and

1 without collusion.

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

4 SUBCHAPTER G

5 PENNSYLVANIA STATEWIDE RADIO NETWORK

6 Sec.

7 4371. Definitions.

8 4372. Administration of PA-STARNet.

9 4373. PA-STARNet Committee.

10 § 4371. Definitions.

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

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

19 "Commissioner." The Commissioner of Pennsylvania State
20 Police.

21 "Committee." The PA-STARNet Committee established under
22 section 4373 (relating to PA-STARNet Committee).

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

26 "First responder." An individual who in the early stages of
27 an incident is responsible for the protection and preservation
28 of life, property, evidence and the environment, including
29 emergency response providers as that term is defined in 6 U.S.C.
30 § 1101 (relating to definitions).

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

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

14 "Public safety communications." The means and methods for
15 transmitting and receiving information necessary for the conduct
16 of services rendered by or through Federal, State or local
17 government entities in support of the protection and
18 preservation of life, property and natural resources, as
19 prescribed by law.

20 "State police." The Pennsylvania State Police.
21 § 4372. Administration of PA-STARNet.

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

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

- 28 (1) the benefit of the participating agencies;
29 (2) the support of effective communications at critical
30 public events; and

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

3 (c) Policies and procedures.--The State police shall
4 establish policies and procedures for the specification,
5 procurement, development, testing, configuration, operations,
6 use, replacement and maintenance of PA-STARNet resources.
7 § 4373. PA-STARNet Committee.

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

14 Section 2. This act shall take effect immediately.